Dr.WEB®

Enterprise Security Suite

Defend what you create

Installationsanleitung

© Doctor Web, 2015. Alle Rechte vorbehalten

Das im vorliegenden Dokument enthaltene Material ist Eigentum von Doctor Web und dient ausschließlich der persönlichen Nutzung durch Produktkäufer. Kein Teil des vorliegenden Dokumentes dard ohne Quellenangabe weder reproduziert noch auf einer Netzwerkressource untergebracht oder mittels Kommunikationskanäle und Massenmedien verbreitet oder auf jede andere Weise benutzt werden, ausgenommen Nutzung für persönliche Zwecke.

WARENZEICHEN
Dr.Web, SpIDer Mail, SpIDer Guard, CureIt!, CureNet!, AV-Desk und Dr.WEB Logo sind eingetragene Warenzeichen von Doctor Web in Russland und/oder anderen Ländern. Alle sonstigen eingetragenen Warenzeichen, Logos und Firmennamen, die im vorliegenden Dokument erwähnt sind, sind Eigentum ihrer jeweiligen Inhaber.

HAFTUNGSAUSSCHLUSS
Unter keinen Umständen haften Doctor Web und seine Lieferanten für die im vorliegenden Dokument enthaltenen Fehler und/oder Auslassungen sowie für Schäden des Produktkäufers (direkte oder indirekte Schäden einschließlich Gewinnausfälle), die sich dadurch ergeben.

Dr.Web Enterprise Security Suite
Version 10.0
Installationsanleitung
21.07.2015

Doctor Web, Hauptsitz Russland
Tretja ul. Jamskogo polja 2, Gebäude 12A
125124 Moskau
Russische Föderation

Website: www.drweb.com
Telefon: +7 (495) 789-45-87

Nähere Informationen zu den regionalen Vertretungen und Büros finden Sie auf unserer Website

Doctor Web

Doctor Web ist ein russischer Anbieter hauseigener IT-Sicherheitslösungen.

Doctor Web bietet effektive Antivirus- und Antispam-Lösungen sowohl für staatliche Einrichtungen und große Unternehmen als auch für private Benutzer.

Die Antivirensoftware von Dr.Web wird seit 1992 entwickelt. Die Antivirus-Lösungen zeigen immer wieder hervorragende Leistungen bei Entdeckung von Malware und entsprechen den weltweiten Sicherheitsnormen.

Zertifikate und Auszeichnungen sowie umfangreiche Geographie der Benutzer zeugen vom besonderen Vertrauen der Kunden in unsere Produkte.

Wir danken den Benutzern für Unterstützung der Lösungen von Dr.Web-Familie!

Inhaltsverzeichnis

Kapitel 1: Dr.Web Enterprise Security Suite 6

1.1. Einleitung 6

1.2. Symbole und Abkürzungen 7

1.3. Über das Produkt 8

1.4. Systemanforderungen 14

1.5. Lieferumfang 18

1.6. Lizenzierung 19

Kapitel 2: Komponenten von Dr.Web Enterprise Security Suite installieren 21

2.1. Antivirus-Netzwerk erstellen 21

2.2. Installation von Dr.Web Server 21

2.2.1. Dr.Web Server unter Windows® installieren 22

2.2.2. Dr.Web Server unter Betriebssystemen der UNIX®-Familie installieren 29

2.2.3. Zusätzliche Distribution des Dr.Web Servers installieren 30

2.2.4. Browser-Erweiterung für das Dr.Web Sicherheitscenter installieren 31

2.3. Dr.Web Agent installieren 32

2.3.1. Installationsdateien 34

2.3.2. Dr.Web Agent lokal installieren 35

2.3.3. Dr.Web Agent unter Windows® remote installieren 42

2.4. NAP Validator installieren 55

2.5. Proxy-Server installieren 55

Kapitel 3: Komponenten von Dr.Web Enterprise Security Suite deinstallieren 58

3.1. Deinstallieren von Dr.Web Server 58

3.1.1. Dr.Web Server unter Windows® deinstallieren 58

3.1.2. Dr.Web Server unter Betriebssystemen der UNIX®-Familie deinstallieren 58

3.2. Dr.Web Agent deinstallieren 60

3.2.1. Dr.Web Agent unter Windows® deinstallieren 60

3.2.2. Dr.Web Agent über Active Directory deinstallieren 62

3.3. Proxy-Server entfernen 62

Kapitel 4: Komponenten von Dr.Web Enterprise Security Suite aktualisieren 64

4.1. Dr.Web Server unter Windows® aktualisieren 64

4.2. Dr.Web Server unter Betriebssystemen der UNIX®-Familie aktualisieren 68

4.3. Browser-Erweiterung für das Dr.Web Sicherheitscenter aktualisieren 72

4.4. Dr.Web Agents aktualisieren 73

4.4.1. Dr.Web Agents unter Windows® aktualisieren 73

4.4.2. Dr.Web Agents unter Linux, Android und MAC OS X aktualisieren 74

4.5. Proxy-Server aktualisieren 75

Schlagwortregister 76

Kapitel 1: Dr.Web Enterprise Security Suite

1.1. Einleitung

Die Dokumentation für Administratoren eines auf der **Dr.Web® Enterprise Security Suite** basierten Antivirus-Netzwerks enthält sowohl allgemeine als auch detaillierte Informationen über Maßnahmen, mit denen Sie in Ihrem Unternehmen einen effizienten und umfassenden Virenschutz durch **Dr.Web® Enterprise Security Suite** implementieren können.

Die Dokumentation für den Administrator des auf der **Dr.Web® Enterprise Security Suite** basierten Antivirus-Netzwerks besteht aus folgenden Teilen:

1. **Installationsanleitung** (die Datei **drweb-esuite-10-install-manual-de.pdf**)

   Die Installationsanleitung kann für Unternehmensleiter nützlich sein, die über den Erwerb und die Implementierung dieser umfassenden Antivirenlösung entscheiden.

   In der Installationsanleitung wird beschrieben, wie Sie ein Antivirus-Netzwerk einrichten und seine Komponenten richtig installieren können.

2. **Administratorhandbuch** (die Datei **drweb-esuite-10-admin-manual-de.pdf**)
3. **Anhänge** (die Datei **drweb-esuite-10-appendices-de.pdf**)

Diese Administratordokumentation enthält Querverweise auf drei oben erwähnte Teile. Beim Aufrufen dieser Dokumente auf einem lokalen Rechner funktionieren diese Querverweise nur dann, wenn alle drei Dokumente unter ihren ursprünglichen Namen und im gleichen Verzeichnis abgespeichert wurden.

Die Administratordokumentation beinhaltet keine Beschreibung von **Dr.Web** Antivirenpaketen für die zu schützenden Workstations. Alle notwendigen Informationen dazu finden Sie im **Benutzerhandbuch** der jeweiligen **Dr.Web** Antivirenlösung.

Bevor Sie mit dem Lesen der Dokumente beginnen, stellen Sie sicher, dass Sie die aktuellste Ausgabe haben. Alle Handbücher werden ständig aktualisiert. Ihre aktuellsten Versionen können Sie jederzeit auf der offiziellen Website von **Doctor Web** unter http://download.drweb.com/esuite/ abrufen.

1.2. Symbole und Abkürzungen

Symbole

In diesem Administratorhandbuch werden Symbole und Hervorhebungen verwendet, die in der Tabelle 1-1 aufgeführt sind.

Tabelle 1-1: Symbole und Hervorhebungen

Symbol/Hervorhebung	Erläuterung
Beachten Sie, dass	Wichtige Bemerkung oder wichtiger Hinweis.
Achtung	Warnung vor eventuellen Fehlersituationen sowie wichtigen Momenten, die besonderer Aufmerksamkeit bedürfen.
Dr.Web Scanner	Namen von **Dr.Web** Produkten und Komponenten.
Antivirus-Netzwerk	Definition oder Link auf eine Definition.
<IP-address>	Platzhalter.
Abbrechen	Namen von Schaltflächen, Fenstern, Menüpunkten und sonstigen Bestandteilen der Benutzeroberfläche.
STRG	Bezeichnungen von Tastaturtasten.
`C:\Windows\`	Namen von Dateien und Verzeichnissen, Ausschnitte des Programmcodes.
Anhang A	Querverweis auf einen Abschnitt im Handbuch oder Hyperlink auf externe Ressourcen.

Abkürzungen

Im Handbuch werden folgende Abkürzungen bzw. Akronyme ohne nähere Erläuterung verwendet:

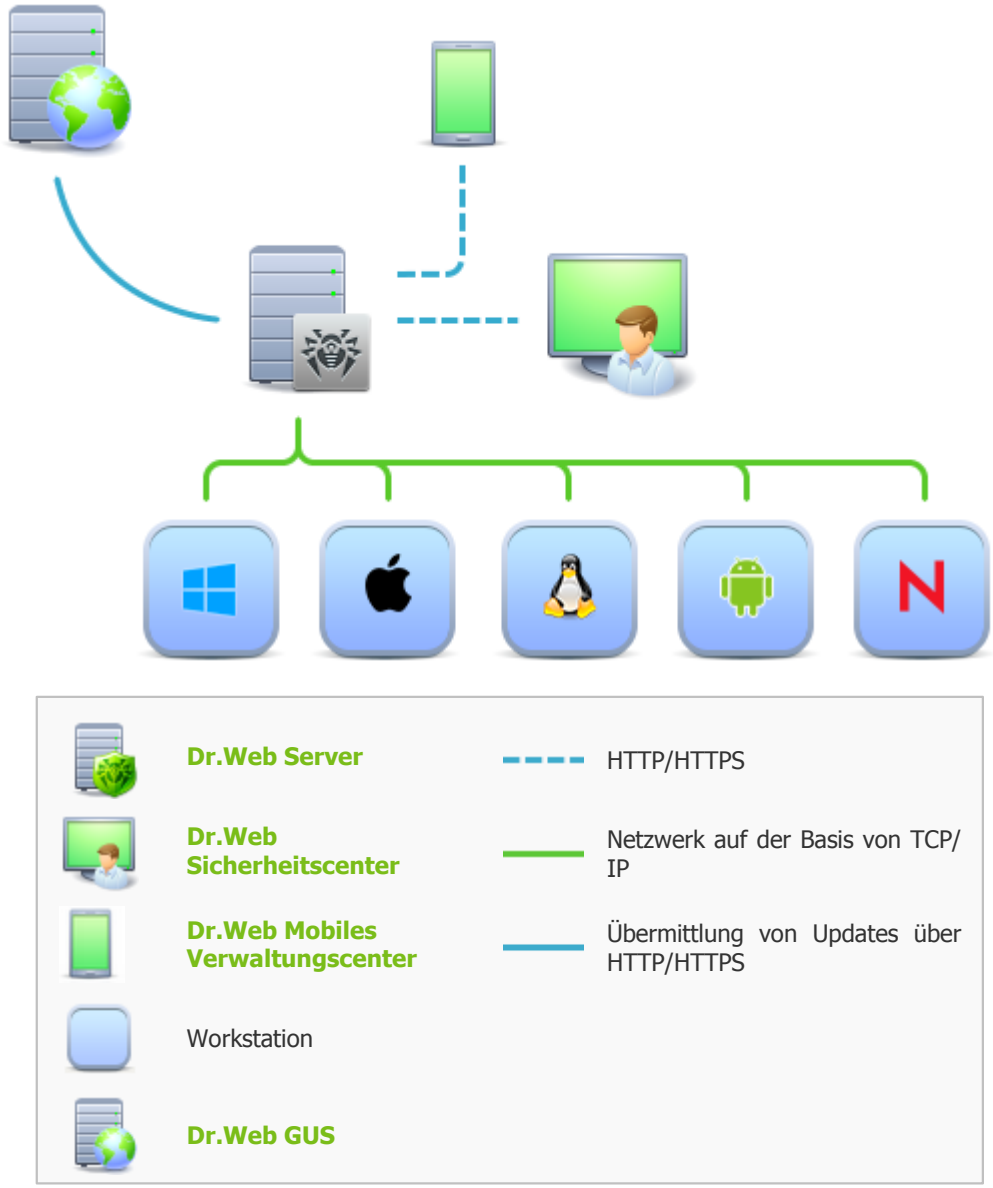
- ACL – Zugriffskontrolllisten (Access Control List)
- CDN – Netzwerk zur Auslieferung von Inhalten (Content Delivery Network)
- DFS – verteiltes Dateisystem (Distributed File System)
- DNS – System der Domänennamen (Domain Name System)
- FQDN – vollständig qualifizierter Domänenname (Fully Qualified Domain Name)
- GUI – grafische Benutzeroberfläche (Graphical User Interface), GUI-Programmversion – eine Version, die GUI-Mittel benutzt
- NAP – Network Access Protection
- MTU – maximale Paketgröße (Maximum Transmission Unit)
- TTL – Lebensdauer des Pakets (Time To Live)
- UDS – UNIX-Domain-Socket (UNIX Domain Socket)
- DB, DBMS – Datenbank, Datenbankmanagementsystem
- **Dr.Web GUS** – **Dr.Web Globales Update-System**
- LAN – lokales Netzwerk
- OS – Betriebssystem
- EBNF – erweiterte Backus-Naur-Form

1.3. Über das Produkt

Dr.Web Enterprise Security Suite bietet einen zuverlässigen zentral administrierbaren Rundumschutz interner Unternehmensnetzwerke, darunter auch mobiler Endgeräte, und privater Rechner von Mitarbeitern vor Schadsoftware jeglicher Art.

Alle Rechner und mobilen Endgeräte, auf denen die Komponenten von **Dr.Web Enterprise Security Suite** installiert sind, bilden ein einheitliches *Antivirus-Netzwerk*.

Das Antivirus-Netzwerk von **Dr.Web <%PRODCUCT%>** verfügt über eine *Client-Server-Architektur.* Seine Komponenten werden auf Rechnern und mobilen Endgeräten der Benutzer und Administratoren sowie auf LAN-Servern installiert. Die Kommunikation zwischen den Komponenten des Antivirus-Netzwerks erfolgt über TCP/IP. Die Antivirensoftware kann dabei auf den zu schützenden Workstations sowohl lokal über LAN, als auch über das Internet installiert (und später verwaltet) werden.



Logische Struktur des Antivirus-Netzwerks

Zentralschutz-Server

Der Zentralschutz-**Server** wird auf einem Rechner des Antivirus-Netzwerks installiert. Dabei kann die Installation nicht nur auf dem Rechner, der als LAN-Server verwendet wird, sondern auch auf einem beliebigen Rechner erfolgen. Die wichtigsten Anforderungen an diesen Rechner finden Sie unter Systemanforderungen.

Die plattformübergreifende Server-Software ermöglicht Ihnen, als **Server** einen Rechner unter einem der folgenden Betriebssysteme zu verwenden:

- Microsoft® Windows® Betriebssysteme
- Betriebssysteme der UNIX-Familie® (Linux®, FreeBSD®, Solaris™)

Auf dem Zentralschutz-**Server** werden Distributionen der Antivirenpakete für verschiedene Betriebssysteme, Updates von Virendatenbanken und Antivirenpaketen, Lizenzschlüssel sowie Einstellungen der Antivirenpakete der zu schützenden Workstations gespeichert. Der **Server** lädt Updates der Antivirenkomponenten von Servern des **Globalen Update-Systems** herunter und überträgt dann diese auf die zu schützenden Workstations.

Dabei können die Workstations bedienenden **Server** in einer hierarchischen Struktur miteinander verbunden werden.

Server unterstützt die Sicherung von kritischen Daten (Datenbanken, Konfigurationsdateien etc.).

Server erstellt ein einheitliches Ereignisprotokoll des Antivirus-Netzwerks.

Einheitliche Datenbank

Die einheitliche Datenbank wird mit dem Zentralschutz-**Server** verbunden. Sie enthält Statistiken zu Ereignissen im Antivirus-Netzwerk, Einstellungen des **Servers**, Parameter der Workstations und installierten Antivirenkomponenten.

Folgende Arten von Datenbanken können verwendet werden:

Eingebettete Datenbank. Zur Verfügung stehen zwei Varianten der Datenbanken, die direkt in den Zentralschutz-**Server** eingebettet sind:

- SQLite2 (InitDB)
- SQLite3

Externe Datenbank. Zur Verfügung stehen integrierte Treiber für die Verbindung der folgenden Datenbanken:

- Oracle
- PostgreSQL
- ODBC-Treiber für die Verbindung anderer Datenbanken, wie etwa Microsoft SQL Server/ Microsoft SQL Server Express

Sie können eine beliebige Datenbank verwenden, die Ihren Bedürfnissen am besten entspricht. Dazu könnte etwa das Folgende zählen: Kapazität der Datenbank, Besonderheiten der Bedienung der Datenbank-Software, Administrationsfunktionen der Datenbank, unternehmensspezifische Vorschriften und Normen.

Zentralschutz-Verwaltungscenter

Das Zentralschutz-**Verwaltungscenter** wird automatisch zusammen mit dem **Server** installiert. Es handelt sich dabei um eine Weboberfläche zur Remote-Verwaltung vom **Server** und Antivirus-Netzwerk. Dies wird durch Ändern der Einstellungen des **Servers** bzw. der Workstations, die auf dem **Server** bzw. auf den Workstations abgespeichert sind, ermöglicht.

Das **Verwaltungscenter** kann auf jedem Rechner geöffnet werden, der über einen Netzwerkzugriff auf den **Server** verfügt. Dabei kann das **Verwaltungscenter** unter fast jedem gängigen Betriebssystem in den folgenden Webbrowsern im vollen Funktionsumfang genutzt werden:

- Windows® Internet Explorer®

- Mozilla® Firefox®
- Google Chrome®

Alle Anforderungen an Webbrowser finden Sie unter Systemanforderungen.

Das Zentralschutz-**Verwaltungscenter** bietet die folgenden Möglichkeiten:

- Schnelle und leichte Installation der **Antivirensoftware** auf Workstations und Remote-Installation auf Workstations unter Windows mithilfe eines Netzwerk-Scanners; Erstellung von Distributionen mit eindeutigen IDs und Einstellungen für die Verbindung mit dem **Server**, was die Installation der **Antivirensoftware** durch Administrator erheblich erleichtert oder eventuelle Installation der **Antivirensoftware** durch Benutzer möglich macht (mehr dazu finden Sie im Abschnitt Dr.Web Agent installieren).
- Vereinfachte Verwaltung von Workstations innerhalb des Antivirus-Netzwerks mithilfe der Gruppenverwaltung.
- Zentrale Verwaltung der Antivirenpakete von Workstations: Löschen sowohl einzelner Komponenten als auch der gesamten **Antivirensoftware** auf Workstations unter Windows; Festlegen der Parameter der Komponenten von Antivirenpaketen; Zuweisen der Rechte zur Einstellung und Verwaltung der Antivirenpakete der Workstations für Benutzer dieser Workstations.
- Zentrale Verwaltung von Scanvorgängen: Zeitgesteuerter Remote-Start eines Suchlaufs oder Remote-Start auf Anforderung des Administrators mithilfe des **Verwaltungscenters**; zentral verwaltetes Festlegen von an die Workstations zu übermittelnden Scan-Parametern, die zum Start eines lokalen Suchlaufs erforderlich sind.
- Anzeige von Statistiken zum Status der zu schützenden Workstations, zu eventuellen Bedrohungen, zum Status der installierten Antivirensoftware und gestarteten Antivirenkomponenten, sowie zur Hardware und Software von Workstations.
- Flexible Verwaltung vom **Server** und Antivirus-Netzwerk durch Einschränkung der Rechte für verschiedene Administratoren; Authentifizierung von Administratoren mithilfe externer Authentifizierungssysteme, wie etwa Active Directory, LDAP, RADIUS, PAM.
- Verwaltung der Lizenzen für die auf Workstations installierte Antivirensoftware und Lizenzvergabe an Workstations, Gruppen von Workstations sowie Lizenzübertragung zwischen mehreren **Servern**, wenn das Antivirus-Netzwerk aus mehreren Servern besteht.
- Umfangreiche Einstellungen zum Konfigurieren vom **Server** und seinen Komponenten, und zwar: Festlegen eines Wartungszeitplans für den **Server**; Durchführen benutzerdefinierter Prozeduren; flexibles Einstellen des Systems zum Aktualisieren aller Komponenten des Antivirus-Netzwerks über das **GUS** und anschließende Übertragung von Updates auf Workstations; Einstellen des Systems zum Benachrichtigen über Ereignisse im Antivirus-Netzwerk mit der Auswahl einer Benachrichtigungsmethode; Konfigurieren von Verbindungen zwischen den Servern, wenn das Antivirus-Netzwerk aus mehreren Servern besteht.

Detaillierte Informationen über die Verwendung der hier beschriebenen Funktionen finden Sie im **Administratorhandbuch**.

Ein Bestandteil des **Dr.Web Sicherheitscenters** ist der **Webserver**, der automatisch zusammen mit dem **Server** installiert wird. Der **Webserver** sorgt für die korrekte Anzeige der Seiten des **Verwaltungscenters** und stabile Client-Netzwerkverbindungen.

Mobiles Zentralschutz-Verwaltungscenter

Das **mobile Verwaltungscenter** ist eine separate Komponente, die auf mobilen Endgeräten unter iOS und Android installiert und betrieben wird. Die wichtigsten Anforderungen an diese App finden Sie unter Systemanforderungen.

Das **mobile Verwaltungscenter** wird mit dem **Server** anhand der Anmeldedaten des Administrators des Antivirus-Netzwerks, eventuell über ein verschlüsseltes Protokoll, verbunden. Das **mobile Verwaltungscenter** hat die wichtigsten Funktionen des **Verwaltungscenters**. Der Administrator des Antivirus-Netzwerks kann dadurch die zu schützenden Workstations direkt über sein mobiles Endgerät verwalten, Statistiken zu Antivirenkomponenten ansehen und Benachrichtigungen für das **mobile Verwaltungscenter** erhalten.

Sie können das **Mobile Verwaltungscenter** über das **Verwaltungscenter** oder direkt aus dem App Store oder Google Play herunterladen.

Schutz von Workstations im Netzwerk

Auf den zu schützenden Rechnern und mobilen Endgeräten des Antivirus-Netzwerks werden jeweils ein Kontrollmodul (**Agent**) und ein betriebssystemabhängiges Antivirenpaket installiert.

Die plattformübergreifende Software ermöglicht einen effektiven Virenschutz der Rechner und mobilen Endgeräte unter den folgenden Betriebssystemen:

- Microsoft® Windows® Betriebssysteme
- Betriebssysteme der UNIX-Familie®
- Mac OS® X
- Android OS
- Novell® NetWare®OS

Geschützt werden können sowohl Rechner der Benutzer als auch LAN-Server, darunter auch das E-Mail-System von Microsoft® Outlook®.

Das Kontrollmodul lädt regelmäßig vom **Server** Updates für die Antivirenkomponenten und Virendatenbanken herunter und übermittelt an den **Server** Informationen über Ereignisse auf der Workstation.

Wenn der Zentralschutz-**Server** nicht verfügbar ist, können die auf den Workstations vorhandenen Virendatenbanken direkt über das **Globale Update-System** aktualisiert werden.

Je nach Betriebssystem können die folgenden Schutzfunktionen zur Verfügung gestellt werden:

Workstations unter Microsoft® Windows®

Virenprüfung

Zeitgesteuertes Scannen oder Scannen auf Anforderung des Benutzers. Ein Scanvorgang (auch mit der Suche nach Rootkits) kann auch über das **Verwaltungscenter** remote ausgelöst werden.

Dateiüberwachung

Permanente Echtzeit-Überprüfung des Dateisystems. Dabei werden alle laufenden Prozesse sowie Dateien überwacht, die auf den Festplatten neu erstellt werden oder auf den Wechseldatenträgern geöffnet werden.

E-Mail-Überwachung

Scannen aller eingehenden und ausgehenden E-Mails, die durch einen E-Mail-Client übertragen werden.

Dabei kann auch ein Spam-Filter verwendet werden (sofern Ihre Lizenz diese Funktion erlaubt).

Webüberwachung

Überprüfung aller HTTP-Zugriffe auf Webseiten. Neutralisieren eventueller Bedrohungen im HTTP-Datenverkehr (z. B. in gesendeten oder empfangenen Dateien) sowie Sperren der Zugriffe auf verdächtige oder unerwünschte Ressourcen.

Office Control

Verwalten des Zugriffs auf lokale Ressourcen bzw. Netzwerkressourcen sowie Webseiten. Diese Funktion sorgt für die Integrität wichtiger Dateien, schützt sie vor dem unbeabsichtigten Ändern oder Infizieren durch Viren und verweigert Mitarbeitern den Zugriff auf unerwünschte Inhalte.

Firewall

Diese Komponente schützt Rechner vor dem unbefugten Zugriff von außen und verhindert den Verlust wichtiger Daten über das Internet. Diese Komponente überwacht Internetverbindungen und Datenübertragungen über das Internet und sperrt verdächtige Verbindungen auf der Paket- und Anwendungsebene.

Quarantäne

Bösartige Programme und verdächtige Objekte werden in einem speziellen Verzeichnis isoliert.

Selbstschutz

Diese Komponente schützt die Dateien und Verzeichnisse von **Dr.Web Enterprise Security Suite** vor dem unbefugten oder unbeabsichtigten Löschen oder Ändern durch Benutzer bzw. bösartige Programme. Beim aktivierten Selbstschutz können nur **Dr.Web** Prozesse auf die Dateien und Verzeichnisse von **Dr.Web Enterprise Security Suite** zugreifen.

Präventivschutz

Diese Komponente sorgt für eine frühzeitige Erkennung eventueller Bedrohungen. Dabei werden Zugriffe auf kritische Objekte des Betriebssystems, Treiberladung, automatisch gestartete Programme, laufende Systemdienste und Prozesse überwacht und beim Virenfund gesperrt.

Workstations unter UNIX®

Virenprüfung

Zeitgesteuertes Scannen oder Scannen auf Anforderung des Benutzers. Ein Scanvorgang kann auch über das **Verwaltungscenter** remote ausgelöst werden.

Dateiüberwachung

Permanente Echtzeit-Überprüfung des Dateisystems. Dabei werden alle laufenden Prozesse sowie Dateien überwacht, die auf den Festplatten neu erstellt werden oder auf den Wechseldatenträgern geöffnet werden.

Webüberwachung

Überprüfung aller HTTP-Zugriffe auf Webseiten. Neutralisieren eventueller Bedrohungen im HTTP-Datenverkehr (z. B. in gesendeten oder empfangenen Dateien) sowie Sperren der Zugriffe auf verdächtige oder unerwünschte Ressourcen.

Quarantäne

Bösartige Programme und verdächtige Objekte werden in einem speziellen Verzeichnis isoliert.

Workstations unter Mac OS® X

Virenprüfung

Zeitgesteuertes Scannen oder Scannen auf Anforderung des Benutzers. Ein Scanvorgang kann auch über das **Verwaltungscenter** remote ausgelöst werden.

Dateiüberwachung

Permanente Echtzeit-Überprüfung des Dateisystems. Dabei werden alle laufenden Prozesse sowie Dateien überwacht, die auf den Festplatten neu erstellt werden oder auf den Wechseldatenträgern geöffnet werden.

Quarantäne

Bösartige Programme und verdächtige Objekte werden in einem speziellen Verzeichnis isoliert.

Mobile Endgeräte unter Android OS

Virenprüfung

Mobile Endgeräte werden auf Anforderung des Benutzers oder zeitgesteuert gescannt. Ein Scanvorgang kann auch über das **Verwaltungscenter** remote gestartet werden.

Dateiüberwachung

Permanentes Echtzeit-Scannen des Dateisystems. Dabei werden auch alle Dateien gescannt, die im Speicher des mobilen Endgeräts abgespeichert werden.

Anruf- und SMS-Filter

Bei der Anruf- und SMS-Filterung werden alle unerwünschten SMS-Nachrichten und Anrufe blockiert, wie z. B. SMS-Werbung oder SMS-Nachrichten und Anrufe von unbekannten Telefonnummern und Kontakten.

Diebstahlschutz

Mit dieser Technologie können Sie Ihre verlorenen bzw. gestohlenen mobilen Endgeräte schnell lokalisieren und sperren.

Eingeschränkter Zugriff auf Internet-Ressourcen

Ein intelligenter URL-Filter schützt Nutzer der mobilen Endgeräte vor unerwünschten Internet-Ressourcen.

Firewall

Diese Komponente schützt Ihr mobiles Endgerät vor dem unbefugten Zugriff von außen und verhindert den Verlust wichtiger Daten über das Netzwerk. Diese Komponente überwacht Internetverbindungen und Datenübertragungen über das Internet und sperrt verdächtige Verbindungen auf der Paket- und Anwendungsebene.

Sicherheits-Auditor

Mit diesem Feature können Sie Ihr mobiles Endgerät auf Sicherheitslücken oder andere sicherheitsrelevante Probleme überprüfen und sie bei Bedarf rechtzeitig beheben.

Anwendungsstart-Steuerung

Diese Komponente verhindert den Start der Anwendungen, die in der Liste vertrauter Anwendungen des mobilen Endgeräts nicht eingetragen sind.

Server unter Novell® NetWare®

Virenprüfung

Zeitgesteuertes Scannen oder Scannen auf Anforderung des Benutzers.

Dateiüberwachung

Permanente Echtzeit-Überprüfung des Dateisystems. Dabei werden alle laufenden Prozesse sowie Dateien überwacht, die auf den Festplatten neu erstellt werden oder auf den Wechseldatenträgern geöffnet werden.

Kommunikation zwischen Komponenten des Antivirus-Netzwerks

Zum Sichern einer stabilen Kommunikation zwischen Komponenten des Antivirus-Netzwerks werden die folgenden Techniken verwendet

Dr.Web Proxy-Server

Der Proxy-Server kann optional ins Antivirus-Netzwerk integriert werden. Der **Proxy-Server** dient hauptsächlich dazu, eine sichere Kommunikation zwischen dem **Server** und Workstations zu gewährleisten, wenn keine direkte Verbindung hergestellt werden kann. Das kann der Fall sein, wenn sich der **Server** und Workstations in verschiedenen Netzwerken befinden, sodass kein Paketrouting möglich ist. Durch das Zwischenspeichern kann außerdem der Netzwerkdatenverkehr verringert und die Zeit der Update-Verteilung verkürzt werden.

Datenverkehr-Kompression

Bei der Kommunikation zwischen den Komponenten des Antivirus-Netzwerks kommen besondere Komprimierungsalgorithmen zum Einsatz, die den Netzwerkdatenverkehr minimal halten.

Verschlüsselung des Datenverkehrs

Bei der Kommunikation zwischen den Komponenten des Antivirus-Netzwerks besteht es die Möglichkeit, den Datenverkehr zu verschlüsseln. Dadurch kann ein besseres Schutzniveau erzielt werden.

Zusätzliche Funktionen

NAP Validator

NAP Validator ist als optionale Komponente verfügbar und ermöglicht, die Microsoft-Technologie des Netzwerkzugriffsschutzes (NAP) zur Diagnose der auf den Workstations installierten Software zu verwenden. Dadurch können Sie sicherstellen, dass Workstations im Netzwerk den definierten Integritätsanforderungen entsprechen.

Repository Lader

Dr.Web Repository Lader ist als optionales Programm verfügbar und ermöglicht, Produkte von **Dr.Web Enterprise Security Suite** über das **Globale Update-System** herunterzuladen. Sie können dieses Tool auch dazu verwenden, um Updates für Produkte von **Dr.Web Enterprise Security Suite** herunterzuladen und sie anschließend auf einen **Server** zu übertragen, der über keine Internetverbindung verfügt.

1.4. Systemanforderungen

Damit Sie Dr.Web Enterprise Security Suite installieren und sicher betreiben können, müssen folgende Voraussetzungen erfüllt sein:

- **Dr.Web Server** muss auf einem Rechner mit Internetzugang installiert werden, um Updates über das **Dr.Web GUS** (Globale Update-System) automatisch herunterladen zu können.

Updates können an die **Server** ohne Internetverbindung übermittelt werden. Beim Antivirus-Netzwerk mit mehreren Servern können Updates nur von einem der **Server** direkt über das **GUS** heruntergeladen werden. Von diesem Server aus werden dann sie auf die anderen **Server** übertragen. Bei dem anderen Verfahren zur Update-Verbreitung wird der **Dr.Web Repository Loader** zum Herunterladen der Updates über das **GUS** verwendet. Einmal heruntergeladen, werden sie dann auf die **Server** übertragen.

- Workstations im Antivirus-Netzwerk müssen über einen Zugriff auf den **Dr.Web Server** oder **Proxy-Server** verfügen.
- Damit Antivirenkomponenten gemeinsam ordnungsgemäß funktionieren können, müssen auf den verwendeten Rechnern die folgenden Ports und Sockets geöffnet sein:

Portnummer	Protokolle	Richtung von Verbindungen	Zweck
2193	TCP	• Eingehende, ausgehende Verbindungen des **Servers** und **Proxy-Servers** • Ausgehende Verbindungen des **Dr.Web Agents**	Für Verbindung der Antivirenkomponenten mit dem **Server** und Kommunikation zwischen Servern. Die Ports werden auch vom **Proxy-Server** zur Verbindung mit Clients verwendet.
	UDP	Eingehende, ausgehende Verbindungen	Für den **Netzwerk-Scanner**.
139, 445	TCP	• Eingehende Verbindungen des **Servers** • Eingehende, ausgehende Verbindungen des **Dr.Web Agents** • Eingehende Verbindungen des Rechners, auf dem das **Verwaltungscenter** geöffnet wird	Für den **Netzwerk-Installer**.
	UDP	Eingehende, ausgehende Verbindungen	
9080	HTTP	• Eingehende Verbindungen des **Servers**	Für das **Dr.Web Sicherheitscenter**.

Portnummer	Protokolle	Richtung von Verbindungen	Zweck
9081	HTTPS	• Eingehende Verbindungen des Rechners, auf dem das **Verwaltungscenter** geöffnet wird	
10101	TCP		Für das Dienstprogramm zur Ferndiagnose des **Servers**.
80	HTTP	Ausgehende Verbindungen	Für das Herunterladen von Updates über das **GUS**.
443	HTTPS		

Beachten Sie, dass in den Versionen des **Servers 4.XX** für die Verbindung der Antivirenkomponenten mit dem **Server** der Port `2371` verwendet wurde. In der Version **10.0** wird dieser Port nicht mehr unterstützt.

Für den Dr.Web Server ist das Folgende erforderlich:

Komponente	Anforderungen
Prozessor und Betriebssystem	Folgende Betriebssysteme werden unterstützt, sofern sie auf den Rechnern mit entsprechender CPU-Leistung installiert sind: ◆ CPU mit Befehlssatzerweiterung SSE2 und 1,3 GHz Taktfrequenz oder besser: • Microsoft Windows • Linux • FreeBSD • Solaris x86-Version ◆ CPU V9 UltraSPARC IIIi oder besser: • Solaris Sparc Die vollständige Liste unterstützter Betriebssysteme finden Sie im Dokument **Anhänge**, im Anhang A.
RAM	• Mindestens: 1 GB • Empfohlen: 2 GB und mehr
Freier Speicherplatz	Mindestens 12 GB: bis 8 GB für integrierte Datenbank (Installationsverzeichnis), bis 4 GB in dem temporären Systemverzeichnis (für Arbeitsdateien). Je nach Einstellungen des **Servers** kann mehr freier Speicherplatz zum Speichern temporärer Dateien benötigt werden. Dazu zählen u. a. individuelle Installationspakete der **Agents** (jeweils ca. 8,5 MB) im Unterverzeichnis `var\installers-cache` des Installationsverzeichnisses vom **Dr.Web Server**. Bei der Installation vom **Server** muss mindestens 1,2 GB freier Speicherplatz für die Basisdistribution und 2,5 GB für die zusätzliche Distribution für den Start des Installationsprogramms und zum Entpacken der temporären Dateien auf dem Systemlaufwerk des Rechners unter Windows bzw. im Verzeichnis `/var/tmp` des Rechners unter einem Betriebssystem der UNIX-Familie (bzw. in einem anderen Verzeichnis für temporäre Dateien, wenn dieses als ihr neuer Speicherort definiert wurde) verfügbar sein. Dabei ist es nicht relevant, wo der **Server** selbst installiert wurde.
Sonstiges	Bei der Installation des **Dr.Web Servers** auf dem Rechner unter einem Betriebssystem der UNIX-Familie müssen folgende Bibliotheken vorhanden sein: `lsb 3.0` oder höher, `glibc 2.7` oder höher. Für Datenbanken des **PostgreSQL**-Datenbankmanagementsystems sind auch `libpq`-Bibliotheken erforderlich. Für Datenbanken des **Oracle**-Datenbankmanagementsystems sind auch `libaio`-Bibliotheken erforderlich.

Komponente	Anforderungen
	Darüber hinaus sind für FreeBSD die `compat-8x`-Bibliotheken erforderlich.

Für den Dr.Web Proxy-Server sind die folgenden Komponenten erforderlich:

Komponente	Anforderung
Prozessor	Intel® Pentium® III mit 667 MHz Taktfrequenz oder besser
RAM	Mindestens 1 GB
Freier Speicherplatz	Mindestens 1 GB
Betriebssystem	• Microsoft Windows • Linux • FreeBSD • Solaris Die vollständige Liste unterstützter Betriebssysteme finden Sie im Dokument **Anhänge**, im Anhang A.
Sonstiges	Bei der Installation des **Proxy-Servers** sind für Betriebssysteme der UNIX-Familie die folgenden Bibliotheken erforderlich: `lsb 3` oder höher.

Für das Dr.Web Sicherheitscenter ist das Folgende erforderlich:

- Einer der folgenden Webbrowser: Windows Internet Explorer 8 oder höher, Mozilla Firefox 25 oder höher, Google Chrome 30 oder höher

  Webbrowser Opera® 10 oder neuer, Safari® 4 oder neuer werden auch unterstützt. Dabei aber kann der volle Funktionsumfang nicht garantiert werden.

  Der volle Funktionsumfang vom **Verwaltungscenter** bei der Verwendung von Windows Internet Explorer 8 mit der aktivierten Option *Verstärkte Sicherheitskonfiguration für Internet Explorer* kann nicht garantiert werden.

  Bei der Installation des **Servers** auf einem Rechner, im wessen Namen das Zeichen „_" (Unterstrich) enthalten ist, kann der **Server** über das **Verwaltungscenter** im Windows Internet Explorer nicht gesteuert werden.

  In diesem Fall sollten Sie einen anderen Webbrowser wählen.

  Für einen korrekten Betrieb vom **Verwaltungscenter** im Windows Internet Explorer muss die IP-Adresse und/oder der DNS-Name des Rechners, auf dem der **Dr.Web Server** installiert ist, zu vertrauenswürdigen Websites des Webbrowsers hinzugefügt werden, in dem das **Verwaltungscenter** geöffnet wird.

  Damit das **Verwaltungscenter** über das Menü **Start** korrekt geöffnet wird, müssen folgende Einstellungen für den Windows Internet Explorer unter Windows 8 und Windows Server 2012 mit Kacheloberfläche festgelegt werden: **Internetoptionen** → **Programme** → **Internet Explorer wird geöffnet** – hier ist die Option **Immer mit Internet Explorer auf dem Desktop** zu aktivieren.

- Die **Browser-Erweiterung für Dr.Web Sicherheitscenter** ist für die vollwertige Nutzung des **Verwaltungscenters** erforderlich. Die Erweiterung wird zusammen mit der Distribution des **Servers** mitgeliefert und auf Anforderung des Webbrowsers bei der Arbeit mit den Elementen des **Verwaltungscenters** installiert, die das Laden der Erweiterung benötigen (für den **Netzwerk-Scanner**, bei der Remote-Installation von Antivirenkomponenten).

Um die **Browser-Erweiterung für Dr.Web Sicherheitscenter** verwenden zu können, brauchen Sie Administratorrechte (root) auf der Seite des **Netzwerk-Scanners** sowohl unter Windows als auch unter Betriebssystemen der GNU/Linux-Familie.

Bei der Verwendung des Safari-Browsers ist die **Browser-Erweiterung für das Dr.Web Sicherheitscenter** nur für Versionen unter Windows verfügbar.

Die **Browser-Erweiterung für das Dr.Web Sicherheitscenter** unterstützt Mozilla Firefox, Opera und Chrome für Windows oder Betriebssysteme der Linux-Familie.

- Die empfohlene Bildschirmauflösung für die optimale Anzeige des **Verwaltungscenters** beträgt 1280x1024 Pixel.

Für das Dr.Web Mobile Verwaltungscenter sind die folgenden Komponenten erforderlich:

Anforderungen unterscheiden sich je nach Betriebssystem des mobilen Geräts:

- iOS:

Komponente	Anforderung
Betriebssystem	iOS® 7 und höher
Gerät	Apple® iPhone® Apple® iPad®

- Android:

Komponente	Anforderung
Betriebssystem	Android 4.0 und höher

Für NAP ist das Folgende erforderlich:

Für Server:

- Windows Server 2008

Für Agents:

- Windows XP SP3, Windows Vista, Windows Server 2008

Für den Dr.Web Agent sowie die Vollversion des Antivirenpakets ist das Folgende erforderlich:

Die tatsächlichen Anforderungen variieren je nach Betriebssystem, auf dem die Antivirenlösung installiert wird (die vollständige Liste unterstützter Betriebssysteme finden Sie im Anhang A. Vollständige Liste unterstützter Betriebssysteme):

- Microsoft Windows:

Komponente	Anforderung
Prozessor	CPU mit 1 GHz Taktfrequenz oder besser
Freies RAM	Mindestens 512 MB
Freier Speicherplatz	Mindestens 1 GB für ausführbare Dateien, Protokolle und temporäre Dateien
Sonstiges	1. Für die korrekte Anzeige der Kontexthilfe des **Dr.Web Agents für Windows** ist der Windows® Internet Explorer® 6.0 oder neuer erforderlich. 2. Für das Plug-In **Dr.Web für Outlook** ist ein installierter Microsoft Outlook Client aus dem MS-Office-Paket erforderlich:

Komponente	Anforderung
	◆ Outlook 2000 (Outlook 9) ◆ Outlook 2002 (Outlook 10 oder Outlook XP) ◆ Office Outlook 2003 (Outlook 11) ◆ Office Outlook 2007 (Outlook 12) ◆ Office Outlook 2010 (Outlook 14) ◆ Office Outlook 2013 (Outlook 15)

- Betriebssysteme der Linux-Familie

Komponente	Anforderung
Prozessor	32-Bit-Prozessor (IA-32, x86) und 64-Bit-Prozessor (x86-64, x64, amd64) auf der Intel-Plattform
Freies RAM	Mindestens 512 MB
Freier Speicherplatz	Mindestens 400 MB freier Speicherplatz auf dem Volume, auf dem sich Verzeichnisse des **Antivirenprogramms** befinden.

- Mac OS X: Konfigurationsanforderungen entsprechen den Anforderungen für das Betriebssystem
- Android: Konfigurationsanforderungen entsprechen den Anforderungen für das Betriebssystem
- Novell Netware: Konfigurationsanforderungen entsprechen den Anforderungen für das Betriebssystem

Auf den Workstations des Antivirus-Netzwerks, das mithilfe von **Dr.Web ESS** verwaltet wird, darf keine andere Antivirensoftware installiert werden (darunter auch andere Versionen der **Dr.Web** Antivirensoftware).

Funktionen der **Agents** werden im Benutzerhandbuch für das jeweilige Betriebssystem beschrieben.

1.5. Lieferumfang

Die Distribution von Dr.Web Enterprise Security Suite wird je nach Betriebssystem des ausgewählten Dr.Web Servers geliefert:

1. Für Betriebssysteme der UNIX-Familie – als `.run`-Dateien für die Installation der folgenden Komponenten:
   - Basisdistribution des **Dr.Web Servers**
   - Zusätzliche Distribution des **Dr.Web Servers**
   - **Proxy-Server**
2. Für Microsoft Windows – als ausführbare Dateien des Installations-Assistenten der folgenden Komponenten:
   - Basisdistribution des **Dr.Web Servers**
   - Zusätzliche Distribution des **Dr.Web Servers**
   - **Proxy-Server**
   - **Dr.Web Agent** für Active Directory
   - Dienstprogramm für die Modifizierung des Active Directory-Schemas
   - Dienstprogramm für die Änderung der Attribute von Active Directory-Objekten
   - **NAP Validator**

Die Distribution des Dr.Web Servers besteht aus zwei Paketen:

1. *Basisdistribution*. Das ist die Hauptdistribution für die Installation des **Dr.Web Servers**. Ihr Inhalt entspricht dem Inhalt der Distribution der alten Versionen von **Dr.Web Enterprise Security Suite**.

   Die Basisdistribution wird auch dazu verwendet, um den **Dr.Web Server** zu installieren, der nur Antivirenpakete für Windows-Workstations enthält.

2. *Zusätzliche Distribution (extra)*. Diese beinhaltet Distributionen sämtlicher Unternehmensprodukte, die für die Installation auf Workstations unter allen unterstützten Betriebssystemen zur Verfügung gestellt werden.

   Dieser Typ der Distribution wird als Ergänzung auf den Rechnern mit bereits installierter *Basisdistribution* des **Dr.Web Servers** installiert.

Der Typ des Installationspakets der zusätzlichen Distribution muss dem der Basisdistribution entsprechen.

Die Basis-Distribution des Dr.Web Servers beinhaltet die folgenden Komponenten:

- Software des **Dr.Web Servers** für das jeweilige Betriebssystem
- Software von **Dr.Web Agents** und Antivirenpaketen für unterstützte Betriebssysteme
- Software des **Dr.Web Sicherheitscenters**
- Virendatenbanken
- Browser-Erweiterung für das **Dr.Web Sicherheitscenter**
- Browser-Erweiterung für **Dr.Web Server FrontDoor**
- Dokumentationen, Muster und Beispiele

Mit der Distribution werden auch Seriennummern mitgeliefert. Nach deren Registrierung erhalten Sie Lizenzschlüsseldateien.

1.6. Lizenzierung

Die Nutzung von **Dr.Web Enterprise Security Suite** wird anhand von Lizenzschlüsseldateien geregelt.

Jede Schlüsseldatei wird durch eine digitale Signatur vor unbefugten Änderungen geschützt. Durch eventuelle Bearbeitung wird die Datei nicht mehr gültig. Um eine zufällige Beschädigung der Datei zu vermeiden, dürfen Sie Ihre Schlüsseldatei nicht bearbeiten und/oder nach ihrem Öffnen in einem Texteditor speichern.

Der Umfang und der Preis einer Lizenz zur Nutzung der Antivirenlösung **Dr.Web Enterprise Security Suite** hängen von der Anzahl der zu schützenden Workstations innerhalb des Netzwerks ab (einschließlich Servern, die im Netzwerk von **Dr.Web Enterprise Security Suite** geschützt werden).

Teilen Sie unbedingt beim Kauf von **Dr.Web Enterprise Security Suite** dem Verkäufer der Lizenz diese Informationen mit. Der Endpreis der Lizenz hängt nicht von der Anzahl der verwendeten **Dr.Web Server** ab.

Informationen zu Besonderheiten der Lizenzierung sowie der Nutzung der Schlüsseldateien für ein bereits bestehendes Antivirus-Netzwerk finden Sie in **dem Administratorhandbuch**, dem Abschnitt Lizenz-Manager.

Die Lizenzschlüsseldatei kann beim Kauf zum Lieferumfang von **Dr.Web Enterprise Security Suite** gehören. In der Regel aber werden nur Seriennummern geliefert.

Die Lizenzschlüsseldatei wird an den Benutzer nach der Registrierung der Seriennummer auf der speziellen Webseite per E-Mail versendet (die Registrierung erfolgt unter http://products.drweb.com/register/, sofern keine andere Adresse auf der Registrierungskarte, die dem Produkt beigefügt wird, angegeben wurde). Besuchen Sie diese Webseite, füllen Sie das Formular mit Angaben zum Käufer aus und geben Sie ins entsprechende Feld eine Seriennummer (diese ist auf der Registrierungskarte angegeben) ein. Das Archiv mit Schlüsseldateien wird an die von Ihnen angegebene E-Mail-Adresse gesendet. Alternativ können Sie dieses Archiv direkt von der Webseite herunterladen.

Schlüsseldateien werden an den Benutzer als ZIP-Archive gesendet, die eine oder mehrere Schlüsseldateien für die zu schützenden Workstations enthalten.

Benutzer können Schlüsseldateien auf eine der folgenden Weisen erhalten:

- Per E-Mail (in der Regel nach der Registrierung auf der Webseite, siehe oben).
- Mit der Distribution des Produkts, sofern Lizenzdateien zum Distributionsumfang des Produkts gehören.
- Als Dateien auf einem separaten Datenträger.

Wir empfehlen Ihnen, Ihre Lizenzschlüsseldatei bis zum Ablauf ihrer Gültigkeitsdauer aufzubewahren und sie bei einer erneuten Installation bzw. Wiederherstellung von Programmkomponenten wieder zu verwenden. Bei Verlust der Lizenzschlüsseldatei können Sie das Registrierungsverfahren auf der oben genannten Webseite wiederholen und eine neue Lizenzschlüsseldatei erhalten. Dabei müssen Sie die gleiche Seriennummer und die gleichen Angaben zum Käufer angeben, die Sie bei der ersten Registrierung angegeben haben. Sie dürfen lediglich eine andere E-Mail-Adresse angeben. In diesem Fall wird Ihre Lizenzschlüsseldatei an die neue E-Mail-Adresse gesendet.

Um sich mit dem **Antivirenprogramm** vertraut zu machen, können Sie Demoschlüsseldateien verwenden. Solche Schlüsseldateien gewährleisten einen vollen Funktionsumfang der Hauptkomponenten, haben aber eine beschränkte Gültigkeitsdauer. Um Demoschlüsseldateien zu erhalten, füllen Sie das entsprechende Formular unter https://download.drweb.com/demoreq/biz/ aus. Ihre Anfrage wird individuell von uns geprüft. Wenn Ihre Anfrage positiv bescheidet wird, senden wir ein Archiv mit Schlüsseldateien an die von Ihnen angegebene E-Mail-Adresse.

Informationen zur Verwendung dieser Schlüsseldateien beim Installieren des Programms finden Sie im Dokument im Abschnitt Dr.Web Server installieren.

Kapitel 2: Komponenten von Dr.Web Enterprise Security Suite installieren

2.1. Antivirus-Netzwerk erstellen

So erstellen Sie ein Antivirus-Netzwerk

1. Erstellen Sie einen Plan des Antivirus-Netzwerks und schließen Sie darin alle zu schützenden Rechner ein. Wählen Sie einen oder mehrere Rechner aus, die als **Dr.Web Server** verwendet werden.
2. Installieren Sie die Software des **Dr.Web Servers** (gleichzeitig wird auch das **Dr.Web Sicherheitscenter** installiert) auf dem gewählten Rechner oder auf den gewählten Rechnern.
3. Aktualisieren Sie Produkte des Repository des **Servers** mithilfe des **Verwaltungscenters**.
4. Konfigurieren Sie die Software der Workstations und des **Servers** (der **Server**).
5. Installieren Sie bei Bedarf einen **Proxy-Server** und stellen Sie ihn entsprechend ein.
6. Installieren Sie auf den Workstations die Software des **Dr.Web Agents**.

Sobald die **Agents** auf den Rechnern installiert sind, stellen sie eine Verbindung mit dem **Server** automatisch her. Die Autorisierung der Antivirus-Workstations auf dem **Server** erfolgt gemäß der von Ihnen ausgewählten Richtlinie (mehr dazu finden Sie im **Administratorhandbuch** unter Verbindungsrichtlinie für Workstations).

7. Konfigurieren Sie über das **Verwaltungscenter** notwendige Module und anschließend starten Sie diese.

Bei der Planung der Netzwerkstruktur müssen Sie einen Rechner auswählen, der als **Dr.Web Server** verwendet wird.

Dr.Web Server kann nicht nur auf dem Rechner, der als LAN-Server verwendet wird, sondern auch auf einem beliebigen Rechner installiert werden. Die wichtigsten Anforderungen an diesen Rechner finden Sie im Abschnitt Systemanforderungen.

Das **Verwaltungscenter** kann nicht nur auf dem Rechner, auf dem der **Server** installiert ist, sondern auch auf jedem anderen Rechner aufgerufen werden, vorausgesetzt dass es zwischen diesem Rechner und dem Rechner, auf dem der **Server** installiert ist, eine sichere Netzwerkkonnektivität besteht.

Das Antivirus-Netzwerk kann aus mehreren **Dr.Web Servern** bestehen. Besonderheiten dieser Netzwerkkonfiguration werden im **Administratorhandbuch** unter Besonderheiten eines Netzwerks mit mehreren Servern näher beschrieben.

Bei der Installation des **Dr.Web Servers** und **Dr.Web Agents** brauchen Sie nur einmal auf die entsprechenden Rechner (physisch oder über Remoteverwaltungstools) zuzugreifen. Alle weiteren Aktionen werden am Arbeitsplatz des Administrators des Antivirus-Netzwerks (auch am Rechner außerhalb des lokalen Netzwerks) durchgeführt und benötigen keinen Zugriff auf den **Dr.Web Server** oder die Workstations.

2.2. Installation von Dr.Web Server

Die Installation des **Dr.Web Servers** ist der erste Schritt zum Einrichten eines Antivirus-Netzwerks. Alle anderen Komponenten des Antivirus-Netzwerks können nicht installiert werden, bis die Installation des Servers erfolgreich abgeschlossen ist.

Die Installation des vollständigen Pakets vom Dr.Web Server besteht aus zwei Phasen:

1. Installation der *Basisdistribution*. Die Basisdistribution wird auch dazu verwendet, um den **Dr.Web Server** zu installieren, der nur Antivirenpakete für Windows-Workstations enthält.
2. Installation der *zusätzlichen Distribution (extra)*. Die zusätzliche Distribution (extra) beinhaltet Distributionen aller anderen Unternehmensprodukte, die für die Installation auf Workstations unter allen unterstützten Betriebssystemen zur Verfügung gestellt werden. Dieser Typ der Distribution wird als Ergänzung auf den Rechnern mit der bereits installierten Distribution des **Dr.Web Servers** installiert.

Die Installation des **Dr.Web Servers** hängt von der zu installierenden Version des **Servers** (Windows oder UNIX-artige Betriebssysteme) ab und erfolgt jeweils unterschiedlich.

Alle Einstellungen, die bei der Installation festgelegt werden, können später beim Betrieb des **Servers** vom Administrator des Antivirus-Netzwerks jederzeit geändert werden.

Wenn Sie die Software des **Servers** bereits installiert haben, wechseln Sie dann zum Abschnitt Dr.Web Server unter Windows® aktualisieren oder Dr.Web Server unter Betriebssystemen der UNIX®-Familie aktualisieren.

Falls Sie vor der Installation der **Server**-Software einen bereits installierten **Server** deinstalliert haben, wird der Inhalt des Repository bei der Installation gelöscht und dessen neue Version installiert. Wenn das Repository einer vorherigen Version aus einem Grund nicht gelöscht wurde, müssen Sie den ganzen Inhalt des Repository vor der Installation einer neuen **Server**-Version manuell löschen und das Repository nach der Installation des **Servers** vollständig aktualisieren.

Die Sprache des Installationsverzeichnisnamens vom **Server** muss der Sprache entsprechen, die in den Windows-Spracheinstellungen für Unicode-inkompatible Programme festgelegt ist. Anderenfalls ist die Installation des **Servers** nicht möglich.

Die besagte Voraussetzung gilt nicht für die englische Sprache.

Zusammen mit dem **Dr.Web Server** wird automatisch das **Dr.Web Sicherheitscenter** installiert. Es dient zur Verwaltung des Antivirus-Netzwerks und zum Konfigurieren des **Servers**.

Standardmäßig wird der **Dr.Web** Server nach der Installation auf den Rechnern unter Windows automatisch gestartet. Unter Betriebssystemen der UNIX-Familie muss er manuell gestartet werden.

Nach der Installation des **Dr.Web Servers** müssen Sie umgehend den öffentlichen Schlüssel (`drwcsd.pub`) an die folgende E-Mail-Adresse von **Doctor Web** register@avdesk.com senden.

2.2.1. Dr.Web Server unter Windows® installieren

Im Nachfolgenden wird beschrieben, wie Sie den **Dr.Web Server** unter Windows installieren können.

Bevor Sie mit der Installation des Dr.Web Servers beginnen, lesen Sie die folgenden Informationen aufmerksam durch:

Die Distributionsdatei sowie andere Dateien, die bei Installation des Programms notwendig sind, müssen sich auf den lokalen Laufwerken desjenigen Rechners befinden, auf dem die Software des **Servers** installiert wird. Die Zugriffsrechte sind so einzustellen, dass diese Dateien für den **LOCALSYSTEM**-Benutzer verfügbar sind.

Die Installation des **Dr.Web Servers** muss von einem Benutzer mit Administratorrechten durchgeführt werden.

Nach der Installation des **Dr.Web Servers** müssen alle Komponenten von **Dr.Web Enterprise Security Suite** aktualisiert werden (mehr dazu finden Sie im **Administratorhandbuch** unter Komponenten von Dr.Web Enterprise Security Suite manuell aktualisieren).

Wenn Sie eine externe Datenbank verwenden, müssen Sie im Voraus eine Datenbank erstellen und einen entsprechenden Treiber konfigurieren (mehr dazu finden Sie im Dokument **Anhänge** unter Anhang B. Einstellungen des DBMS. Einstellungen für DBMS-spezifische Treiber).

Das Installationsprogramm des **Servers** unterstützt die benutzerdefinierte Installation. Um einzelne Komponenten, wie etwa DBMS-spezifische Treiber, hinzuzufügen bzw. zu löschen, starten Sie das Installationsprogramm des **Servers** und wählen Sie **Ändern** aus.

In der Abbildung 2-1 finden Sie das Flussdiagramm für die Installation des **Dr.Web Servers** mithilfe eines Installationsprogramms. Jeder Schritt wird unten ausführlich beschrieben.

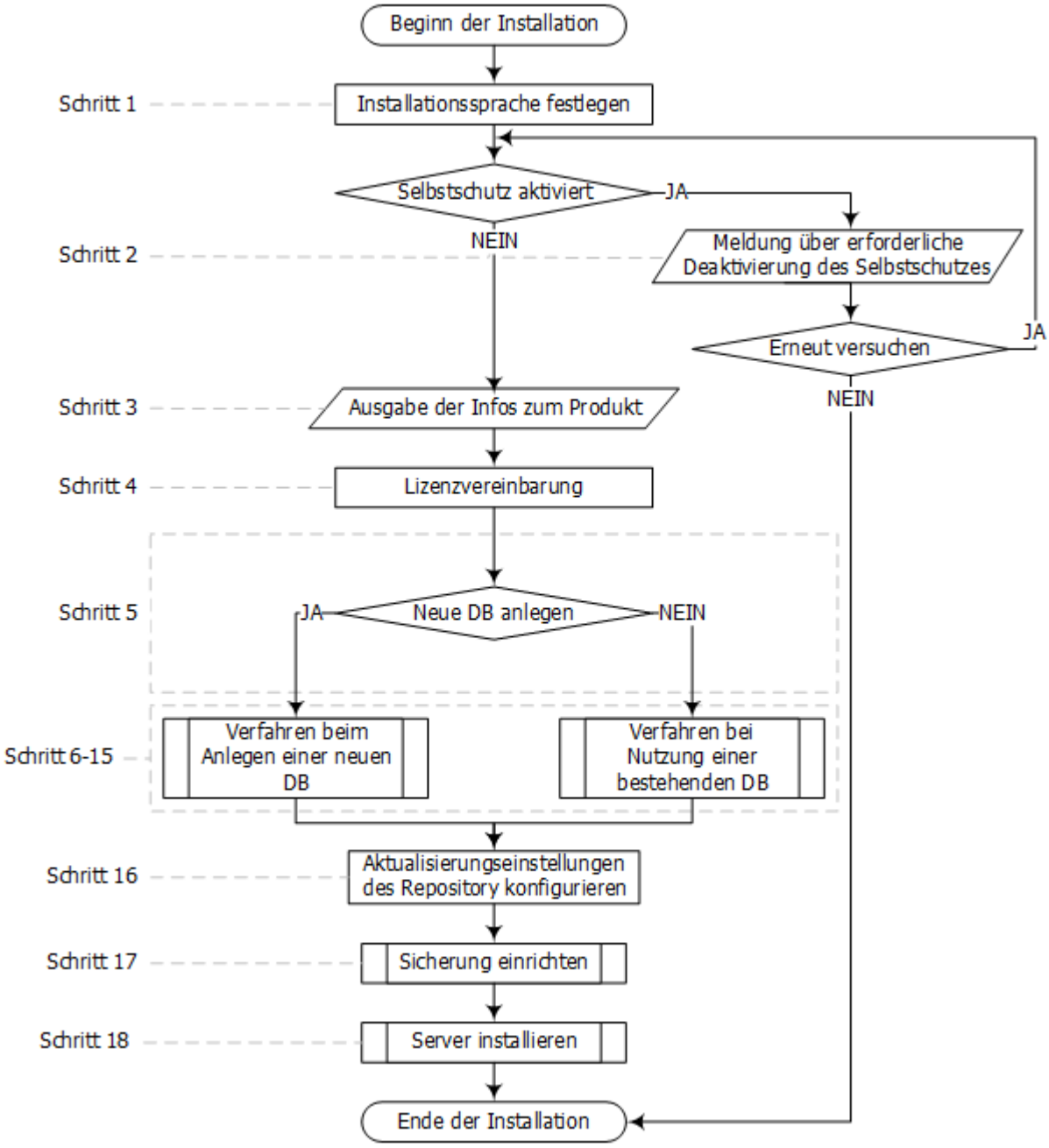


Abbildung 2-1: Ablaufplan für die Installation des Dr.Web Servers (um zur gewünschten Beschreibung zu gelangen, klicken Sie auf das jeweilige Element)

Das Flussdiagramm enthält drei integrierte Prozeduren. Die Prozedur **Installation des Servers** (Schritt 18) benötigt keinen Eingriff durch Benutzer (s. die Beschreibung unten) und wird direkt durch das Installationsprogramm ausgeführt.

Flussdiagramme der Prozeduren **bei der Erstellung einer neuen DB** und **bei der Verwendung einer bestehenden DB** sind in den Abbildungen unten zu sehen.

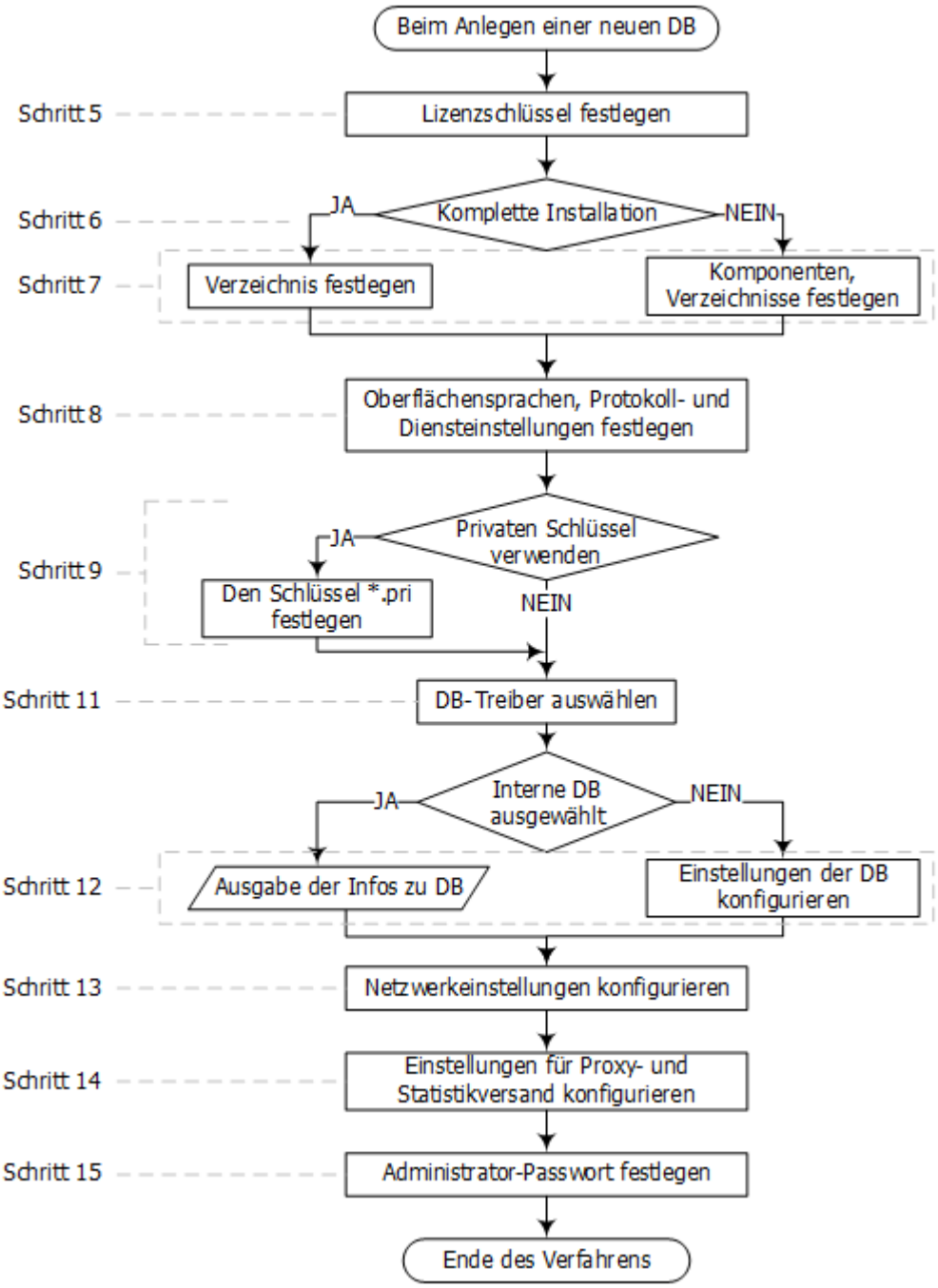


Abbildung 2-2: Ablaufplan für die Installation bei der Erstellung einer neuen DB (um zur gewünschten Beschreibung zu gelangen, klicken Sie auf das jeweilige Element)

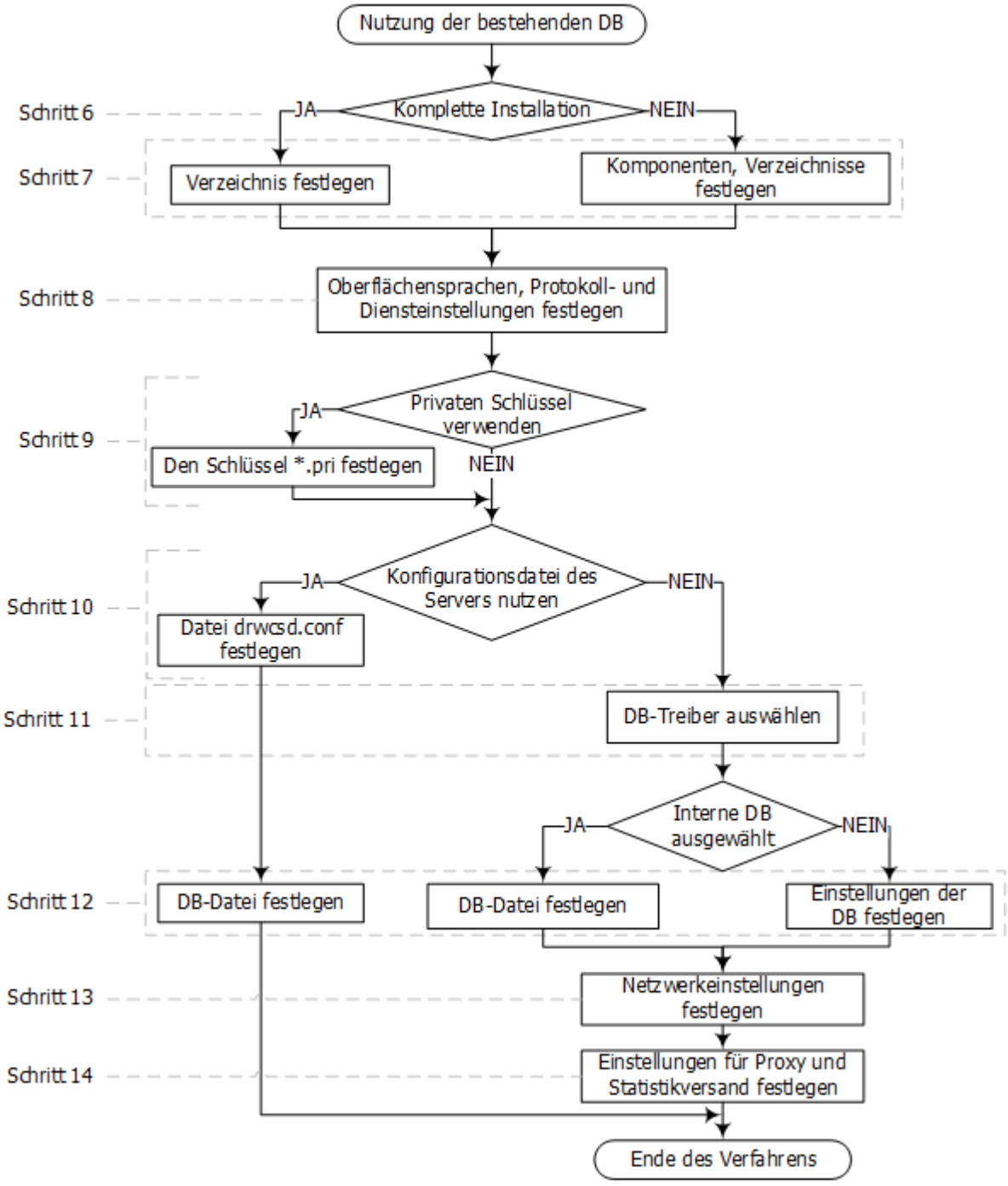


Abbildung 2-3. Ablaufplan für die Installation des Dr.Web Servers bei der Verwendung einer bestehenden DB (um zur gewünschten Beschreibung zu gelangen, klicken Sie auf das jeweilige Element)

So installieren Sie den Dr.Web Server auf einem Rechner unter Windows

1. Starten Sie die Distributionsdatei. Es öffnet sich das Fenster zur Auswahl der Sprache für den Installationsprozess. Wählen Sie **Deutsch** und klicken Sie auf **Weiter**.
2. Wenn auf dem Rechner, auf dem Sie den **Dr.Web Server** installieren möchten, bereits ein **Dr.Web Agent** mit der aktivierten Selbstschutzfunktion installiert ist, wird eine Meldung über die aktivierte **Dr.Web** Selbstschutzfunktion angezeigt. Deaktivieren Sie diese Komponente des **Agents** und klicken Sie auf **OK**, um den Vorgang fortzusetzen, bzw. auf **Abbrechen**, um die Installation des **Servers** zu beenden.
3. Es öffnet sich das Fenster **InstallShield Wizard** mit Informationen zum zu installierenden Produkt. Klicken Sie die Schaltfläche **Weiter** an.

4. Als nächstes Fenster erscheint die Lizenzvereinbarung. Nachdem Sie sich mit den Bedingungen der Lizenzvereinbarung vertraut gemacht haben, wählen Sie **Ich akzeptiere die Bedingungen der Lizenzvereinbarung** aus und klicken Sie auf **Weiter**.
5. Es öffnet sich das Fenster zur Auswahl der Datenbank für das Antivirus-Netzwerk und der Lizenzschlüsseldatei, sofern dies notwendig ist.

   Bei der Erstinstalltion des **Servers** wählen Sie **Neue Datenbank erstellen** aus. Geben Sie im Feld **Dr.Web Lizenzschlüssel** eine Lizenzschlüsseldatei an oder lassen Sie es leer. Lizenzschlüssel können nach der Installation des **Servers** mithilfe vom Lizenzmanager hinzugefügt werden.

   Wenn Sie die Datenbank des bereits installierten **Servers** verwenden möchten, wählen Sie **Vorhandene Datenbank benutzen** aus. Die Datenbankdatei können Sie später angeben (s. den Schritt **10**).

   Um sich mit dem Produkt vertraut zu machen, können Sie Demoschlüsseldateien benutzen. Klicken Sie auf **Demoschlüssel**, um auf die Webseite von **Doctor Web** zu gelangen und Demoschlüsseldateien zu erhalten (s. Demoschlüsseldateien).

   Klicken Sie auf **Weiter**.

6. Es öffnet sich das Fenster zur Auswahl der Installationsart. Wenn Sie **Vollständig** auswählen, werden alle Komponenten des **Dr.Web Servers** installiert. Wenn Sie die **Benutzerdefiniert** auswählen, können Sie im nächsten Schritt nur die gewünschten Komponenten zur Installation auswählen. Nachdem Sie die gewünschte Installationsart ausgewählt haben, klicken Sie auf **Weiter**.

   Wenn Sie als externe Datenbank eine ODBC-Datenbank für Oracle verwenden möchten, wählen Sie die Option **Benutzerdefiniert** aus und deaktivieren Sie im geöffneten Fenster die Installation des integrierten Clients für Oracle-DBMS (im Abschnitt **Database support** – **Oracle database driver**).

   Anderenfalls kann auf die Oracle-Datenbank aufgrund eventueller Probleme durch inkompatible Bibliotheken nicht zugegriffen werden.

7. Wenn Sie im vorherigen Schritt die Installationsart **Vollständig** ausgewählt haben, öffnet sich das Fenster zur Auswahl des Installationsverzeichnisses. Wenn Sie das Standard-Installationsverzeichnis ändern möchten, klicken Sie auf **Ändern** und wählen Sie das gewünschte Installationsverzeichnis aus. Klicken Sie dann auf **Weiter**.

   Wenn Sie im vorherigen Schritt die Installationsart **Benutzerdefiniert** ausgewählt haben, öffnet sich das Fenster zur Auswahl der zu installierenden Komponenten und Verzeichnisse. Im Kontextmenü der Komponenten können Sie die Installationsart jeder Komponente ändern: Jede Komponente kann auf einem lokalen Rechner bzw. zum Ausführen über das Netzwerk (nicht bei allen Komponenten möglich) installiert werden. Sie können auch die Installation einer Komponente abbrechen. Wenn Sie das Standard-Installationsverzeichnis der in der Liste ausgewählten Komponente ändern möchten, klicken Sie auf **Ändern** und geben Sie das gewünschte Installationsverzeichnis an. Klicken Sie anschließend auf **Weiter**.

8. Wählen Sie im geöffneten Fenster die Sprachen aus, die für die Benutzeroberfläche der Komponenten des Antivirus-Netzwerks verwendet werden sollen:
   - Wählen Sie in der Dropdown-Liste **Sprache der Dr.Web Server Benutzeroberfläche** Ihre Standardsprache für die Benutzeroberfläche des **Dr.Web Sicherheitscenters** aus.
   - Wählen Sie in der Dropdown-Liste **Sprache der Dr.Web Agent Benutzeroberfläche** Ihre Standardsprache für die Benutzeroberfläche des **Dr.Web Agents** aus.

   Ändern Sie bei Bedarf die Berechtigungen und den Namen der freigegebenen Ressource für das Installationsverzeichnis des **Agents** (standardmäßig wird der ausgeblendete Name der freigegebenen Ressource festgelegt).

   Aktivieren Sie das Kontrollkästchen **Den Dr.Web Server-Dienst während der Installation starten**, um den **Server** nach der Installation automatisch starten zu lassen.

Um Einstellungen zum Protokollieren der Installation und dem Betrieb des **Servers** festzulegen, klicken Sie auf **Einstellen** und legen Sie die gewünschten Einstellungen fest.

Aktivieren Sie das Kontrollkästchen **Serverports und -schnittstellen den Firewall Ausnahmen hinzufügen**, um den **Server** zur Ausnahmenliste der Windows-Firewall hinzuzufügen.

9. Bei der Erstinstallation des **Servers** klicken Sie im geöffneten Fenster auf **Weiter**. Die Verschlüsselungsschlüssel werden automatisch bei der Installation generiert.

   Wenn Sie den **Server** für ein bereits vorhandenes Antivirus-Netzwerk installieren, aktivieren Sie das Kontrollkästchen **Vorhandene kryptographische Schlüssel verwenden** und geben Sie einen privaten Schlüssel an. Danach wird der öffentliche Schlüssel generiert (der Inhalt des öffentlichen Schlüssels ist mit dem Inhalt des vorherigen öffentlichen Schlüssels identisch). Dadurch können die bereits installierten **Agents** einen neuen **Server** erkennen. Anderenfalls müssen Sie nach der Installation den neuen öffentlichen Schlüssel in alle Workstations kopieren, auf denen **Dr.Web Agents** bereits installiert wurden.

10. Wenn Sie im Schritt **5** eine bestehende Datenbank ausgewählt haben, öffnet sich ein Dialogfeld, in dem Sie die im Voraus vorbereitete Konfigurationsdatei des **Servers** angeben können.

    In den nächsten Dialogfeldern werden die wichtigsten Einstellungen des **Servers** festgelegt (mehr dazu finden Sie im **Administratorhandbuch** unter Dr.Web Server konfigurieren).

11. Im Dialogfeld für die Konfiguration der Datenbank werden die Einstellungen für die verwendete Datenbank festgelegt. Diese Einstellungen hängen von dem im Schritt **5** ausgewählten Typ der Datenbank sowie von der Verfügbarkeit der im Schritt **9** festgelegten Konfigurationsdatei des **Servers** ab.

    Wenn Sie eine neue Datenbank erstellen möchten oder keine Konfigurationsdatei des **Servers** (für die vorhandene Datenbank) angegeben haben, wählen Sie einen Treiber, der verwendet werden soll. Bei der Auswahl **SQLite3-Datenbanktreiber** (standardmäßig gewählt) oder **IntDB Datenbanktreiber** müssen Sie die integrierten Datenbanken des **Dr.Web Servers** verwenden. Bei anderen Optionen müssen Sie die entsprechenden externen Datenbanken verwenden. Alle Einstellungen für das jeweilige DBMS werden im Anhang detailliert beschrieben (s. das Dokument **Anhänge** unter Anhang B. Einstellungen des DBMS. Einstellungen für DBMS-spezifische Treiber).

    Klicken Sie auf **Weiter**.

12. Wenn Sie die Option **SQLite3-Datenbanktreiber** oder **IntDB Datenbanktreiber** zum Erstellen einer neuen Datenbank im vorherigen Schritt ausgewählt haben, werden im nächsten Fenster die Informationen zur zu erstellenden Datenbank angezeigt.

    Wenn Sie bei der Verwendung einer vorhandenen Datenbank im vorherigen Schritt eine Konfigurationsdatei für den **Server** festgelegt haben oder **SQLite3-Datenbanktreiber** bzw. **IntDB Datenbanktreiber** ausgewählt haben, müssen Sie in diesem Fenster eine Datenbankdatei angeben. Klicken Sie dafür auf **Durchsuchen**. Aktivieren Sie das Kontrollkästchen **Überprüfung der internen Datenbank während der Installation starten**, um die Integrität der Datenbank bei der Installation des **Servers** zu überprüfen.

    Wenn Sie im vorherigen Schritt eine Variante der externen DBMS angegeben haben, müssen Sie im nächsten Fenster die Einstellungen für den Zugriff auf die Datenbank festlegen.

13. Wenn Sie sich im Schritt **5** für das Erstellen einer neuen Datenbank entschieden haben oder im Schritt **9** (für die vorhandene Datenbank) keine Konfigurationsdatei für den vorher installierten **Server** festgelegt haben, erscheint das Dialogfeld zum Konfigurieren des Netzwerks. In diesem Dialogfeld wird das Netzwerkprotokoll des **Servers** konfiguriert. Sie dürfen nur ein Netzwerkprotokoll konfigurieren. Zusätzliche Netzwerkprotokolle können später konfiguriert werden.

    Legen Sie in den Feldern **Schnittstelle** und **Port** die entsprechenden Werte für den Zugriff auf den **Server** fest. Standardmäßig wird die Schnittstelle `0.0.0.0` festgelegt, d.h. der Zugriff auf den **Server** ist über alle Schnittstellen möglich.

Standardmäßig wird der Port 2193 verwendet.

Bitte beachten Sie: In den Versionen des **Servers 4.XX** wurde der Port 2371 verwendet. In der Version **10.0** wird dieser Port nicht mehr unterstützt.

Die Adressen müssen im Format von Netzwerkadressen angegeben werden. Die erlaubten Schreibweisen finden Sie im Dokument **Anhänge** unter Anhang E. Spezifikation zur Schreibweise von Netzwerkadressen.

Um den lokalen Zugriff auf den **Server** einzuschränken, aktivieren Sie das Kontrollkästchen **Eingeschränkter Zugriff auf Dr.Web Server.** In diesem Fall können **Installationsprogramme der Agents**, **Agents** und andere **Server** (wenn ein auf der **Dr.Web Enterprise Security Suite** basiertes Antivirus-Netzwerk bereits vorhanden ist) auf den **Server** nicht zugreifen. Später können Sie die Einstellungen über das Menü des **VerwaltungscentersAdministrierung** im Punkt **Dr.Web Server-Konfiguration** auf der Registerkarte **Module** jederzeit ändern.

Aktivieren Sie das Kontrollkästchen **Server-Suchdienst**, wenn Sie möchten, dass der **Server** auf Multicast- oder Broadcastanforderungen anderer **Server** antwortet.

Um die Standard-Netzwerkkonfiguration festzulegen, klicken Sie unterhalb des Fensters auf **Standard**. Wenn Sie den **Server** nur an die interne Netzwerkschnittstelle 127.0.0.1 binden möchten, klicken Sie auf **Eingeschränkt**. Bei diesen Einstellungen kann der **Server** nur über das **Verwaltungscenter**, das auf dem gleichen Rechner geöffnet ist, verwaltet werden. Außerdem kann sich mit diesem **Server** nur derjenige **Agent** verbinden, der auf dem gleichen Rechner gestartet wurde. Nachdem der **Server** konfiguriert wurde, können Sie diese Netzwerkeinstellungen jederzeit ändern.

Klicken Sie auf **Weiter**.

14. Wenn Sie sich im Schritt **5** für das Erstellen einer neuen Datenbank entschieden haben oder im Schritt **9** (für eine bestehende Datenbank) keine Konfigurationsdatei für den vorher installierten **Server** festgelegt haben, werden Sie im nächsten Fenster aufgefordert, Statistiken zu Bedrohungen an **Doctor Web** zu versenden. Dafür aktivieren Sie das Kontrollkästchen **Statistik versenden**. Im Feld **Absenden der Statistiken (Min.)** legen Sie das Intervall (in Minuten) zum Versenden der Statistiken.

    Wenn Sie einen Proxy-Server verwenden, können Sie in diesem Feld auch seine Einstellungen festlegen. Um einen Proxy-Server verwenden zu können, aktivieren Sie das Kontrollkästchen **Proxy verwenden**.

    Das Kontrollkästchen **Proxy verwenden** kann nur dann aktiviert werden, wenn es im Installationsverzeichnis des **Servers** keine Konfigurationsdateien von älteren Installationen gibt.

    Legen Sie für die Verbindung mit dem Proxy-Server die folgenden Einstellungen fest:

    - **Proxy-Server** – die Adresse des Proxy-Servers (Pflichtfeld).
    - **Benutzer**, **Passwort** – Benutzername und Passwort für den Zugriff auf den Proxy-Server, wenn der Proxy-Server die Authentifizierung unterstützt.
    - In der Dropdown-Liste **Authentifizierungsmethode** wählen Sie eine Authentifizierungsmethode, falls der Proxy-Server die Authentifizierung unterstützt.

    Klicken Sie auf **Weiter**.

15. Wenn Sie im Schritt **5** für das Erstellen einer neuen Datenbank entschieden haben, legen Sie in diesem Fenster ein Passwort für den Administrator des Antivirus-Netzwerks, der standardmäßig unter dem Namen **admin** erstellt wird und den Vollzugriff auf das Antivirus-Netzwerk besitzt.

    Klicken Sie auf **Weiter**.

16. Wir empfehlen Ihnen, im geöffneten Fenster die Aktualisierung des Repository bei der Installation des **Servers** zu aktivieren. Aktivieren Sie dafür das Kontrollkästchen **Repository aktualisieren**.

    Klicken Sie auf **Weiter**.

17. Wenn der Rechner, auf dem der **Server** installiert werden soll, zur einer Active Directory-Domäne gehört, werden Sie im nächsten Schritt aufgefordert, **Dr.Web Server** in der Active Directory-Domäne zu registrieren. Bei der Registrierung in der Active Directory-Domäne wird auf dem DNS-Server ein SRV-Eintrag erstellt, der dem **Dr.Web Server** entspricht. Über diesen SRV-Eintrag können dann Clients auf den **Dr.Web Server** zugreifen.

    Legen Sie zur Registrierung die folgenden Parameter fest:

    - Aktivieren Sie das Kontrollkästchen **Den Dienst bei Active Directory registrieren**.
    - Geben Sie in den Feldern **Benutzername** und **Passwort** die Anmeldedaten des Administrators der Active Directory-Domäne an.
    - Geben Sie im Feld **Domäne** den Namen der Active Directory-Domäne, in welcher der **Server** registriert werden soll. Wenn keine Domäne angegeben ist, wird die Domäne verwendet, in welcher der Rechner, auf dem die Installation erfolgt, registriert ist.

18. Im nächsten geöffneten Fenster wird das Verzeichnis ausgewählt, in das kritische Daten des **Servers** gemäß dem Aufgabenzeitplan des **Servers** kopiert werden sollen. Um das Standardverzeichnis zu ändern, klicken Sie auf **Durchsuchen** und wählen Sie das gewünschte Verzeichnis aus. Klicken Sie auf **Weiter**.
19. Klicken Sie auf **Installieren**. Weitere Aktionen des Installationsprogramms benötigen keine weiteren Eingriffe durch Benutzer.
20. Nachdem die Installation abgeschlossen ist, klicken Sie auf **Fertig**.

Der **Dr.Web Server** verfügt über keine integrierte Oberfläche. Der **Dr.Web Server** wird in der Regel über das **Verwaltungscenter** verwaltet, das als Oberfläche des **Servers** verwendet wird.

Bei der Installation des **Servers** wird im Windows-Startmenü **Programme** das Verzeichnis **Dr.Web Server** mit den folgenden Elemente zum Konfigurieren und Verwalten des **Servers** erstellt:

- Das Verzeichnis **Serververwaltung** beinhaltet Befehle zum Start, Neustart und Beenden des **Servers**, Befehle zum Konfigurieren der Protokollierung sowie andere Befehle des **Servers**. Ihre detaillierte Beschreibung finden Sie im Dokument **Anhänge** unter H5. Dr.Web Server.
- Der Punkt **Weboberfläche** dient zum Aufrufen vom **Verwaltungscenter** bzw. zur Verbindung mit dem **Server**, der auf diesem Rechner installiert ist (unter http://localhost:9080).
- Der Punkt **Dokumentation** dient zum Öffnen der Administratordokumentation im HTML-Format.

Die Struktur des Installationsverzeichnisses vom **Server** wird im **Administratorhandbuch** unter Dr.Web Server beschrieben.

2.2.2. Dr.Web Server unter Betriebssystemen der UNIX®-Familie installieren

Alle Aktionen bei der Installation müssen über die Konsole vom Super-User (**root**) durchführt werden.

So installieren Sie Dr.Web Server unter Betriebssystemen der UNIX-Familie

1. Um die Installation des Pakets vom **Server** zu starten, führen Sie den folgenden Befehl aus:

   ```
   sh ./<Distributionsdatei>.run
   ```

Das Installationspaket kann alternativ über die Befehlszeile gestartet werden. Entsprechende Schalter finden Sie im Dokument **Anhänge** unter H10. Installationsprogramm des Dr.Web Servers für Betriebssysteme der UNIX®-Familie

Der Standardname vom Administratorkonto des Antivirus-Netzwerks ist **admin**, das Passwort ist **root**.

2. Als nächstes Fenster erscheint die Lizenzvereinbarung. Akzeptieren Sie die Bedienungen der Lizenzvereinbarung, um die Installation fortzusetzen.
3. Wenn Sie gefragt werden, wo die Sicherung angelegt werden soll, legen Sie den Pfad zum gewünschten Verzeichnis fest oder bestätigen Sie das Standard-Sicherungsverzeichnis `/var/tmp/drwcs`.
4. Anschießend wird die Installation der Software durchgeführt. Bei der Installation können Sie aufgefordert werden, Ihre Aktionen als Administrator zu bestätigen.

Bei der Installation der Software unter **FreeBSD** wird das `rc`-Skript `/usr/local/etc/rc.d/drwcsd.sh` erstellt.

Verwenden Sie die folgenden Befehle:

- `/usr/local/etc/rc.d/drwcsd.sh stop` – um den **Server** manuell zu stoppen
- `/usr/local/etc/rc.d/drwcsd.sh start` – um den **Server** manuell zu starten.

Beachten Sie bitte, dass Sie keinen Lizenzschlüssel bei der Installation des **Servers** anzugeben brauchen. Lizenzschlüssel müssen erst nach der Installation des **Servers**, über den Lizenzmanager hinzugefügt werden.

2.2.3. Zusätzliche Distribution des Dr.Web Servers installieren

Die Installation der zusätzlichen Distribution (extra) muss auf dem Rechner durchgeführt werden, auf dem bereits die Basisdistribution des **Dr.Web Servers** installiert wurde. Die Vorgehensweise bei der Installation der Basisdistribution des **Servers** wird im Abschnitt Dr.Web Server unter Windows® installieren und Dr.Web Server unter Windows® installieren beschrieben.

Der Typ des Installationspakets der zusätzlichen Distribution muss dem der Basisdistribution entsprechen.

So installieren Sie die zusätzliche Distribution des Dr.Web Servers auf einem Rechner unter Windows

1. Starten Sie die Distributionsdatei.
2. Es öffnet sich das Fenster **Dr.Web ESuite Extra** mit Informationen zu dem zu installierenden Produkt und mit dem Text der Lizenzvereinbarung. Nachdem Sie sich mit den Bedingungen der Lizenzvereinbarung vertraut gemacht haben, wählen Sie **Ich akzeptiere die Bedingungen der Lizenzvereinbarung** aus und klicken Sie dann auf **Installieren**.
3. Die Installation der zusätzlichen Distribution wird gestartet. Falls keine Fehler auftreten, benötigt sie keine Benutzereingriffe.
4. Nachdem die Installation abgeschlossen ist, klicken Sie auf **Fertig**. Ein Neustart des Rechners ist dabei nicht erforderlich.

So installieren Sie die zusätzliche Distribution des Dr.Web Servers auf einem Rechner unter einem UNIX-artigen Betriebssystem

1. Verwenden Sie zum Starten der Distributionsdatei den folgenden Befehl:

   `sh ./`*`<Distributionsdatei>`*`.run`

2. Als nächstes Fenster erscheint die Lizenzvereinbarung. Akzeptieren Sie die Bedienungen der Lizenzvereinbarung, um die Installation fortzusetzen.

3. Danach wird die Software installiert.

2.2.4. Browser-Erweiterung für das Dr.Web Sicherheitscenter installieren

Die **Browser-Erweiterung für das Dr.Web Sicherheitscenter** unterstützt Mozilla Firefox, Opera und Chrome für Windows oder Betriebssysteme der Linux-Familie.

Die **Browser-Erweiterung für das Dr.Web Sicherheitscenter** sorgt für den vollen Funktionsumfang des **Verwaltungscenters** (s. auch Systemanforderungen an das Dr.Web Sicherheitscenter).

Die Erweiterung wird zusammen mit der Distribution des **Servers** mitgeliefert und kann auf zwei Weisen installiert werden:

1. Automatisch, auf Anforderung des Webbrowsers beim Betrieb des **Verwaltungscenters**, und zwar bei der Verwendung der Elemente, die das Hochladen der Erweiterung (für den **Netzwerk-Scanner**, bei der Remote-Installation der Antivirenkomponenten) benötigen.
2. Manuell, mithilfe des Installationsprogramms der Erweiterung für das **Dr.Web Sicherheitscenter**.

Browser-Erweiterung für das Dr.Web Sicherheitscenter manuell installieren

So laden Sie das Installationsprogramm zur manuellen Installation der Erweiterung für das Dr.Web Sicherheitscenter herunter

1. Öffnen Sie das **Verwaltungscenter**. Wenn die **Browser-Erweiterung für das Dr.Web Sicherheitscenter** für den verwendeten Webbrowser noch nicht installiert ist, erscheint unterhalb des Hauptmenüs eine Aufforderung zum Installieren der Erweiterung.
2. Klicken Sie auf den Link **Browser-Erweiterung für Dr.Web Sicherheitscenter installieren**.

Dr.WEB
Security Control Center extension
Die Browser-Erweiterung für Dr.Web Sicherheitscenter lässt das Dr.Web Sicherheitscenter vollwertig nutzen. Diese Erweiterung enthält einen Portscanner und das Modul zur Remoteinstallation der Antivirus-Software unter Windows OS.
Browser-Erweiterung für Dr.Web Sicherheitscenter für Firefox 37 (x86)
Herunterladen
64-Bit-Version der Browser-Erweiterung für Dr.Web Sicherheitscenter
© Doctor Web, 1992-2015
Datenschutzerklärung

Abbildung 2-4: Bereich zum Herunterladen der Browser-Erweiterung für das Dr.Web Sicherheitscenter

3. Im Bereich zum Herunterladen der Erweiterung wird die Version des aktuellen Webbrowsers sowie die mögliche Bitanzahl (x86 oder x64) der Erweiterung angegeben.

   Unter Betriebssystemen der UNIX-Familie werden Sie aufgefordert, in der Dropdown-Liste die gewünschte Version auszuwählen.

4. Um die Erweiterung herunterzuladen und zu speichern, klicken Sie auf **Herunterladen**. Danach können Sie diese manuell installieren.
5. Um zur Version mit einer anderen Bitanzahl zu wechseln, klicken Sie auf den Link unterhalb der Herunterladen-Schaltfläche. Dadurch können Sie das Installationsprogramm wie im Schritt **4** beschrieben herunterladen.

So installieren Sie die Browser-Erweiterung für das Dr.Web Sicherheitscenter unter Windows

1. Starten Sie die ausführbare Datei. Es öffnet sich das Fenster **InstallShield Wizard** mit Informationen zum zu installierenden Produkt. Klicken Sie die Schaltfläche **Weiter** an.
2. Als nächstes Fenster erscheint die Lizenzvereinbarung. Nachdem Sie sich mit den Bedingungen der Lizenzvereinbarung vertraut gemacht haben, wählen Sie **Ich akzeptiere die Bedingungen der Lizenzvereinbarung** aus und klicken Sie auf **Weiter**.
3. Es öffnet sich das Fenster zur Auswahl des Installationsverzeichnisses. Wenn Sie das Standard-Installationsverzeichnis ändern möchten, klicken Sie auf **Ändern** und wählen Sie das gewünschte Installationsverzeichnis aus. Klicken Sie dann auf **Weiter**.
4. Um mit der Installation zu beginnen, klicken Sie im nächsten Fenster auf **Installieren**. Weitere Aktionen des Installationsprogramms benötigen keine weiteren Eingriffe durch Benutzer.
5. Nachdem die Installation abgeschlossen ist, klicken Sie auf **Fertig**.

So installieren Sie die Browser-Erweiterung für das Dr.Web Sicherheitscenter unter UNIX-basierten Betriebssystemen

Führen Sie den folgenden Befehl aus:

- Für **deb**-Pakete:
  `dpkg -i drweb-esuite-plugins-linux-<Distributionsversion>.deb`
- Für **rpm**-Pakete:
  `rpm -i drweb-esuite-plugins-linux-<Distributionsversion>.rpm`
- Für sonstige Systeme (Pakete **tar.bz2** und **tar.gz**):
  1. Entpacken Sie das Archiv mit der Erweiterung.
  2. Erstellen Sie ein Verzeichnis für die Erweiterung, sofern dieses noch nicht erstellt wurde.

  Zum Beispiel, für Mozilla Firefox Browser: `mkdir /usr/lib/mozilla/plugins`
  3. Kopieren Sie die im Schritt 1 entpackte Bibliothek ins Verzeichnis für die Erweiterung.

  Zum Beispiel, für Mozilla Firefox Browser: `cp libnp*.so /usr/lib/mozilla/plugins`

Starten Sie nach der Installation der **Browser-Erweiterung für das Dr.Web Sicherheitscenter** unter UNIX-artigen Betriebssystemen Ihren Webbrowser neu, falls er bereits ausgeführt wird.

2.3. Dr.Web Agent installieren

Die Installation des **Dr.Web Agents** muss von einem Benutzer mit Administratorrechten durchgeführt werden.

Wenn auf der Workstation bereits ein **Antivirenprogramm** vorhanden ist, müssen Sie vor dem Start der neuen Installation das vorhandene **Antivirenprogramm** deinstallieren.

Dr.Web Agent kann auf einer Workstation über zwei Wege installiert werden:

1. Lokale Installation

Die lokale Installation erfolgt direkt auf einem Rechner oder mobilen Endgerät des Benutzers. Sie kann sowohl vom Benutzer als auch vom Administrator durchgeführt werden.

2. Remote-Installation

   Die Remote-Installation ist nur für Workstations unter Windows möglich und wird vom **Verwaltungscenter** aus über LAN durchgeführt. Die Installation selbst wird vom Administrator des Antivirus-Netzwerks ohne Beteiligung des Benutzers ausgeführt.

Dr.Web Agent auf einer Windows-Workstation mit einem bereits installierten Dr.Web Produkt installieren

Wenn auf der Workstation unter Windows ein eigenständiges **Dr.Web** Produkt der Version **7**/**8**/**9** bereits installiert ist, muss die Installation des **Agents** für **Dr.Web Enterprise Security Suite** der Version **10.0** wie folgt durchgeführt:

- Falls das Installationsprogramm oder Installationspaket vom **Agent** im GUI-Modus auf einer Workstation mit dem bereits installierten eigenständigen Produkt der Version **7.0**/**8.0**/**9.0** ausgeführt wird, wird das Installationsprogramm des installierten Produktes gestartet. Der Benutzer wird dann aufgefordert, den Code zur Bestätigung seiner Aktionen einzugeben und das Produkt zu deinstallieren. Nach dem Neustart der Workstation wird die GUI-Version des Installationsprogramms gestartet, das früher zur Installation des **Agents** für **Dr.Web Enterprise Security Suite** der Version **10.0** gestartet wurde.
- Wird das Installationsprogramm des **Agents** auf einer Workstation mit dem installierten Produkt der Version **7.0**/**8.0**/**9.0** im Hintergrundmodus gestartet, erfolgt keine Aktion. Bei der Remote-Installation sendet das Installationsprogramm ans **Verwaltungscenter** eine Nachricht darüber, dass auf der Workstation ein eigenständiges Produkt anderer Version bereits vorhanden ist. In diesem Fall müssen Sie das eigenständige Produkt manuell entfernen und den **Agent** für **Dr.Web Enterprise Security Suite** der Version **10.0** über eine der vorhandenen Methoden installieren.
- Wird das Installationsprogramm des **Agents** auf einer Workstation mit dem bereits installierten eigenständigen Produkt der Version **9.1** gestartet, wird das installierte Produkt vom eigenständigen Modus in den Zentralschutz-Modus umgeschaltet. Nachdem eine Verbindung mit dem **Server** hergestellt wurde und die Autorisierung erfolgreich durchgeführt wurde, können Updates, neue Einstellungen und die Liste neuer Komponenten übertragen werden. Dabei ist u. U. ein Neustart erforderlich.

Beachten Sie bei der Installation von Dr.Web Agents auf LAN-Servern bzw. Rechnern des Clusters das Folgende:

- Bei der Installation auf den Rechnern, die als Terminalserver (unter Windows sind **Terminal Services** installiert) verwendet werden, sind die **Agents** nur lokal über die **Systemsteuerung** des Windows-Betriebssystems zu installieren, damit die **Agents** in den Terminalsitzungen der Benutzer funktionsfähig bleiben.
- Falls möglich, vermeiden Sie es, die Komponenten **SpIDer Gate**, **Office Control**, **SpIDer Mail** und **Dr.Web Firewall** auf den Servern zu installieren, die wichtige Netzwerkfunktionen (z. B. Funktion eines Domänencontrollers oder Lizenz-Verteilungsservers usw.) übernehmen. Dadurch können Sie eventuelle Konflikte zwischen Netzwerkdiensten und internen Komponenten des **Dr.Web** Antivirenprogramms verhindern.
- Die Installation des **Agents** in einem Cluster muss für jeden Cluster-Knoten separat erfolgen.
- Die Funktionsprinzipien des **Agents** und der Komponenten des Antivirenpakets auf einem Cluster-Knoten sind denen auf einem standardmäßigen LAN-Server ähnlich. Aus diesem Grund ist es nicht empfehlenswert, auf den Cluster-Knoten die Komponenten**SpIDer Gate**, **SpIDer Mail** und **Dr.Web Firewall** zu installieren.
- Wenn der Zugriff auf die Quorum-Ressource im Cluster eingeschränkt ist, ist es empfehlenswert, diese vom Scan durch **SpIDer Guard** auszuschließen. In diesem Fall können Sie Ressourcen mithilfe des **Scanners** manuell oder zeitgesteuert scannen lassen.

2.3.1. Installationsdateien

Installationspaket

Beim Erstellen eines neuen Workstation-Kontos wird im **Verwaltungscenter** ein Installationspaket für den **Dr.Web Agent** generiert. Ein Installationspaket besteht aus dem **Dr.Web Agent** und einem Parametersatz, der Einstellungen für die Verbindung mit dem **Dr.Web Server** und für die Autorisierung am **Dr.Web Server** beinhaltet.

Installationspakete sind für Workstations unter allen Betriebssystemen verfügbar, die von **Dr.Web Enterprise Security Suite** unterstützt werden. Beachten Sie dabei das Folgende:

- Für Workstations unter Windows sind die Installationspakete verfügbar, die im **Verwaltungscenter** auf der Basis des Netzwerk-Installers des **Agents** generiert werden. Alle notwendigen Einstellungen für die Verbindung mit dem **Server** und für die Autorisierung der Workstation am **Server** sind im Installationspaket enthalten.
- Ein Installationspaket für Workstations unter Android, Linux, Mac OS X besteht aus einem Installationsprogramm für den **Agent** und einer Konfigurationsdatei, die alle Einstellungen für die Verbindung mit dem **Server** und für die Autorisierung der Workstation am **Server** enthält.

Um Installationspakete für Nicht-Windows-Betriebssysteme zu erhalten, müssen Sie auch die zusätzliche Distribution (extra) des **Dr.Web Servers** installieren.

Der Link zum Herunterladen des Installationspakets des **Dr.Web Agents** für die jeweilige Workstation ist verfügbar:

1. Sobald die neue Workstation erstellt ist (s. den Schritt **11** im Abschnitt Neues Workstation-Konto erstellen).
2. Zu jeder Zeit, nachdem die Workstation erstellt ist:
   - In den Eigenschaften der Workstation oder
   - im Bereich **Ausgewählte Objekte** bei der Auswahl der Workstation in der hierarchischen Liste.

Installationsprogramm

Das Installationsprogramm des **Agents** unterscheidet sich vom Installationspaket dadurch, dass es über keine Einstellungen für die Verbindung mit dem **Server** und für die Autorisierung der Workstation am **Server** verfügt.

Zur Verfügung stehen die folgenden Typen des Installationsprogramms des **Dr.Web Agents**:

- Für Workstations unter Windows sind zwei Typen des Installationsprogramms verfügbar:
  - *Netzwerk-Installer* `drwinst.exe` sorgt nur für die Installation des **Agents**. Nachdem eine Verbindung mit dem **Server** hergestellt wurde, lädt der **Agent** entsprechende Komponenten des Antivirenpakets herunter und installiert sie. Die Installation des **Agents** mithilfe des Netzwerk-Installers kann sowohl lokal als auch remote erfolgen.

    Der Netzwerk-Installer des **Agents** `drwinst.exe` befindet sich im Verzeichnis `Installer` (dieses ist standardmäßig ein versteckter freigegebener Ordner) des Installationsverzeichnisses vom **Dr.Web Server**. Die Ressource wird im Schritt 8 der Installation des **Dr.Web Servers** freigegeben. Diese Ressource kann nachträglich geändert werden.
  - *Vollversion des Installationsprogramms* `drweb-esuite-agent-full-10.00.0-<Buildversion>-windows.exe` sorgt für die gleichzeitige Installation des **Agents** und Installationspakets.

- Für Workstations unter Android, Linux, Mac OS X ist das Installationsprogramm für den **Dr.Web Agent** verfügbar, das dem Installationsprogramm der eigenständigen Version ähnlich ist.

Installationsprogramme für den **Antivirus** finden Sie auf der Installationsseite des **Dr.Web Sicherheitscenters**.

Um Installationsprogramme für Nicht-Windows-Betriebssysteme und eine vollständige Distribution des Installationsprogramms für Windows-Betriebssysteme zu erhalten, müssen Sie auch die zusätzliche Distribution (extra) des **Dr.Web Servers** installieren.

Installationsseite

Auf der Installationsseite des **Dr.Web Sicherheitscenters** können Sie die folgenden Tools herunterladen:

1. Installationsprogramm des **Dr.Web Agents**.

   Installationsprogramme für Workstations unter allen Betriebssystemen, die **Dr.Web Enterprise Security Suite** unterstützt, befinden sich in Verzeichnissen mit den Namen des jeweiligen Betriebssystems.

2. Öffentlichen Schlüssel `drwcsd.pub`.

Die Installationsseite ist auf jedem Rechner mit dem Netzwerkzugriff auf den **Dr.Web Server** unter der folgenden Adresse verfügbar:

`http://`*<Serveradresse>*`:`*<Portnummer>*`/install/`

Als *<Serveradresse>* geben Sie die IP-Adresse bzw. den DNS-Namen des Rechners an, auf dem der **Dr.Web Server** installiert ist. Als *<Portnummer>* geben Sie die Portnummer `9080` (bzw. `9081` für https) an.

2.3.2. Dr.Web Agent lokal installieren

Die lokale Installation des **Dr.Web Agents** erfolgt direkt auf dem Rechner oder mobilen Endgerät des Benutzers. Sie kann sowohl vom Benutzer als auch vom Administrator durchgeführt werden.

Vor der ersten Installation von **Dr.Web Agents** müssen Sie das **Server**-Repository aktualisieren (mehr dazu finden Sie im **Administratorhandbuch** unter Komponenten von Dr.Web Enterprise Security Suite manuell aktualisieren unter **Auf Updates überprüfen**).

Workstations unter Android, Linux, Mac OS X

Für die lokale Installation des **Dr.Web Agents** auf Workstations unter Android, Linux, Mac OS X stehen die folgenden Tools zur Verfügung:

- Installationspaket, das im **Verwaltungscenter** generiert wurde.
- Installationsprogramm des **Dr.Web Agents**.

Achten Sie bei der Auswahl eines passenden Tools auf die folgenden Besonderheiten:

a) Das generierte Installationspaket enthält das Installationsprogramm des **Dr.Web Agents**, Parameter für die Verbindung mit dem **Server** und für die Autorisierung der Workstation am **Server** werden aber in einer Konfigurationsdatei bereitgestellt.

b) Bei der Verwendung des Installationsprogramms wird nur der **Dr.Web Agent** installiert. Das Tool selbst beinhaltet keine Parameter für die Verbindung mit dem **Server** und für die Autorisierung am **Server**.

Workstations unter Windows

Für die lokale Installation vom **Dr.Web Agent** auf Workstations unter Windows stehen die folgenden Tools zur Verfügung:

- Installationspaket, das im **Verwaltungscenter** generiert wurde.
- Vollversion des Installationsprogramms des **Dr.Web Agents**.
- Netzwerk-Installer des **Dr.Web Agents**.

Achten Sie bei der Auswahl eines passenden Tools auf die folgenden Besonderheiten:

a) Das Installationspaket beinhaltet die Parameter für die Verbindung mit dem **Server** und Autorisierung der Workstation am **Server**. Bei der Verwendung des Installationspakets wird der **Agent** mithilfe des Netzwerk-Installers installiert. Sobald eine Verbindung mit dem **Server** hergestellt ist, lässt der **Agent** Komponenten des Antivirenpakets herunterladen und anschließend installieren.

b) Bei der Verwendung der Vollversion des Installationsprogramms werden der **Agent** und das Antivirenpaket gleichzeitig installiert. Das Tool selbst beinhaltet keine Parameter für die Verbindung mit dem **Server** und für die Autorisierung am **Server**.

c) Der Netzwerk-Installer sorgt nur für die Installation des **Agents**. Nachdem eine Verbindung mit dem **Server** hergestellt ist, lässt der **Agent** entsprechende Komponenten des Antivirenpakets herunterladen und anschließend installieren. Dabei werden keine Parameter für die Verbindung mit dem **Server** und Autorisierung am **Server** bereitgestellt.

Um Installationspakete und Installationsprogramme für Nicht-Windows-Betriebssysteme und die Vollversion des Installationsprogramms für Windows-Betriebssysteme zu erhalten, müssen Sie auch die zusätzliche Distribution (extra) des **Dr.Web Servers** installieren.

Alle Installationsdateien des **Agents** können alternativ über die Befehlszeile ausgeführt werden. Im Dokument **Anhänge** unter H2. Netzwerk-Installer können Sie alle notwendigen Schalter finden.

2.3.2.1. Dr.Web Agent mithilfe des Installationspakets installieren

So installieren Sie Dr.Web Agent mithilfe eines Installationspakets

1. Erstellen Sie auf dem **Dr.Web Server** über das **Verwaltungscenter** ein Konto für den neuen Benutzer.
2. Senden Sie an den Benutzer den Link auf das Installationspaket vom **Dr.Web Agent** für das jeweilige Betriebssystem des Rechners oder mobilen Endgeräts, wenn die Software des **Dr.Web Agents** vom Benutzer installiert werden soll. Falls die Installation auf einer Workstation unter einem Nicht-Windows-Betriebssystem erfolgt, müssen Sie an den Benutzer auch die Konfigurationsdatei mit den Parametern für die Verbindung mit dem **Dr.Web Server** (s. den Schritt **11** beim Erstellen eines neuen Workstation-Kontos) versenden.

Um die Übertragung der Installationsdatei und Konfigurationsdateizu vereinfachen, verwenden Sie die Funktion **Installationsdateien versenden** (mehr Informationen dazu finden Sie im **Administratorhandbuch** unter Installationsdateien versenden). Dadurch können Sie an die gewünschte E-Mail-Adresse eine E-Mail-Nachricht mit angehängten Installationsdateien versenden.

3. Installieren Sie den **Dr.Web Agent** auf der Workstation.

Die lokale Installation vom **Dr.Web Agent** wird im **Benutzerhandbuch** für das jeweilige Betriebssystem detailliert beschrieben.

Die Installation des **Dr.Web Agents** muss von einem Benutzer mit Administratorrechten durchgeführt werden.

Wenn eine Antivirensoftware auf der Workstation bereits installiert ist, versucht das Installationsprogramm vor dem Beginn der Installation diese Software zu entfernen. Wenn dieser Versuch fehlschlägt, muss diese Antivirensoftware vom Benutzer entfernt werden.

4. Legen Sie die Parameter für die Verbindung mit dem **Dr.Web Server** direkt auf der Workstation fest.

Neues Workstation-Konto erstellen

Um ein oder mehrere Konten für neue Benutzer anzulegen, verwenden Sie das **Dr.Web Verwaltungscenter**.

Achten Sie beim Erstellen eines Kontos unbedingt auf den Namen des **Servers**, den in den folgenden Bereichen vom **Verwaltungscenter** angegeben wurde:

1. **Administrierung** > **Konfiguration des Webservers** > das Feld **Server** (wird im Parameter `<server-name />` der Konfigurationsdatei `webmin.conf` gespeichert). Der Wert dieses Parameters wird beim Generieren des Links auf das Installationspaket vom **Agent** verwendet.
   Wenn der Wert dieses Parameters nirgends festgelegt ist, wird der DNS-Name (falls verfügbar) oder die IP-Adresse des Rechners, auf dem das **Verwaltungscenter** aufgerufen wurde, als Name des **Servers** zum Generieren des Links zum Herunterladen des Installationsprogramms vom **Agent** verwendet.
2. **Administrierung** > **Dr.Web Server-Konfiguration von** > Registerkarte **Herunterladen** > das Feld**Server** (wird im Parameter `<name />` der Konfigurationsdatei `download.conf` gespeichert). Der Wert dieses Parameters wird in Installationspaketen des **Agents** verwendet, um einen **Server** zu definieren, mit dem der **Agent** bei der Installation eine Verbindung herstellen soll.
   Wenn der Wert dieses Parameters nirgends festgelegt ist, wird beim Erstellen des Installationspakets vom **Agent** die Adresse des **Servers** verwendet, mit dem das **Verwaltungscenter** verbunden ist. In diesem Fall muss das **Verwaltungscenter** mit dem **Server** über die IP-Adresse für die Domäne verbunden werden, in der das Konto erstellt wird (als Adresse des **Servers** darf nicht ein Loopback mit der Adresse `127.0.0.1` angegeben werden).

So erstellen Sie einen neuen Benutzer über das Dr.Web Sicherheitscenter

1. Wählen Sie im Hauptmenü vom **Verwaltungscenter** den Punkt **Antivirus-Netzwerk**.
2. Klicken Sie auf der Symbolleiste auf **Station oder Gruppe hinzufügen**. Wählen Sie im geöffneten Untermenü **Station erstellen**. Im rechten Fensterbereich vom **Verwaltungscenter** öffnet sich das Panel zum Erstellen eines neuen Benutzerkontos.
3. Geben in das Feld **Anzahl** die Zahl der zu erstellenden Benutzer ein.
4. Im Feld **Identifikator** wird für die erstellte Workstation automatisch eine eindeutige ID generiert. Bei Bedarf kann diese geändert werden.
5. Geben Sie im Feld **Name** einen Namen für die Workstation an, der in der hierarchischen Liste des Antivirus-Netzwerks angezeigt wird. Nachdem die Workstation mit dem **Server** verbunden ist, kann dieser Name automatisch durch den Namen der Workstation ersetzt werden, der lokal festgelegt wurde.
6. In die Felder **Passwort** und **Passwort bestätigen** können Sie das Passwort für den Zugriff auf den **Server** eingeben. Das Passwort wird automatisch generiert, wenn Sie diese Felder leer lassen.

Wenn mehrere Benutzerkonten erstellt werden, werden die Felder **Identifikator**, **Name** und **Passwort** (**Passwort bestätigen**) mit entsprechenden Angaben automatisch ausgefüllt. Beachten Sie dass, sie beim Erstellen von Workstations nicht geändert werden können.

7. Geben Sie im optionalen Feld **Beschreibung** zusätzliche Informationen über den Benutzer an.
8. Im Bereich **Gruppen** werden die Gruppe festgelegt, in welche die zu erstellende Workstation aufgenommen werden soll.
   - In der Liste **Mitgliedschaft** können Sie die benutzerdefinierten Gruppen auswählen, in welche die Workstation aufgenommen werden soll.
     Standardmäßig gehört die Workstation zur Gruppe **Everyone**. Wenn einige benutzerdefinierte Gruppen vorhanden sind, kann die zu erstellende Workstation in diese Gruppen ohne Einschränkung an der Anzahl der Gruppen, zu denen die Workstation gehört, eingeschlossen werden. Aktivieren Sie dafür in der Liste **Mitgliedschaft** die Kontrollkästchen neben den gewünschten benutzerdefinierten Gruppen.

   Die Workstation darf weder aus der Gruppe **Everyone** noch aus der Primärgruppe ausgeschlossen werden.

   Um die Primärgruppe für die Workstation festzulegen, klicken Sie auf das Symbol der gewünschten Gruppe im Bereich **Mitgliedschaft**. Auf dem Symbol der Gruppe wird dabei die Ziffer **1** angezeigt.
9. Füllen Sie bei Bedarf den Bereich **Sicherheit** aus. Alle Einstellungen dieses Bereichs werden im **Administratorhandbuch** unter Sicherheit beschrieben.
10. Füllen Sie bei Bedarf den Bereich **Speicherstelle** aus.
11. Klicken Sie auf **Speichern** in der Ecke oben rechts. Es öffnet sich ein Fenster, das Sie darüber informiert, dass eine neue Workstation erfolgreich erstellt wurde. Das Fenster beinhaltet auch die Identifikationsnummer sowie die folgenden Links:
    - Unter **Installationsdatei** finden Sie einen Link zum Herunterladen vom Installationsprogramm des **Agents**.

      Sobald die neue Workstation eingerichtet ist, aber bevor Sie das jeweilige Betriebssystem der Workstation angeben müssen, werden im Bereich zum Herunterladen der Distribution Links für jedes der von **Dr.Web Enterprise Security Suite** unterstützten Betriebssysteme zur Verfügung gestellt.

      Um Installationspakete für Nicht-Windows-Betriebssysteme zu erhalten, müssen Sie auch die zusätzliche Distribution (extra) des **Dr.Web Servers** installieren.
    - Unter dem Punkt **Konfigurationsdatei** finden Sie einen Link zum Herunterladen der Datei mit den Einstellungen für die Verbindung von Workstations unter Android, MAC OS X und Linux mit dem **Dr.Web Server**.
    - Unter **Passwort** finden Sie das Passwort für den Zugriff auf den **Server**. Um das Passwort anzeigen zu lassen, klicken Sie auf .

      Die entsprechenden Links zum Herunterladen des Installationsprogramms vom **Agent** und der Konfigurationsdatei finden Sie auch in:
      - Eigenschaften der jeweiligen Workstation, nachdem sie eingerichtet ist.
      - Im Bereich **Ausgewählte Objekte** bei der Auswahl der erstellten Workstation in der hierarchischen Liste.
    - In diesem Fenster ist auch die Schaltfläche **Installieren** verfügbar, mit der Sie Dr.Web Agent über das Dr.Web Sicherheitscenter remote installieren können.
12. Die Vorgehensweise bei der Installation des **Dr.Web Agents** wird im **Benutzerhandbuch** für das jeweilige Betriebssystem beschrieben.

Verbindung mit dem Dr.Web Server konfigurieren

- **Workstations unter Windows**

  Bei der Installation des **Dr.Web Agents** mithilfe eines Installationspakets auf Workstations unter Windows brauchen Sie keine zusätzlichen Einstellungen vorzunehmen. Jedes Installationspaket enthält bereits alle notwendigen Einstellungen für die Verbindung mit dem **Server** und für die Autorisierung der Workstation am **Server**. Nachdem die Installation des **Agents** abgeschlossen ist, stellt die Workstation eine Verbindung mit dem **Server** automatisch her.

- **Workstations unter Android**

  1. Rufen Sie auf dem Startbildschirm des mobilen Endgeräts das Menü der Anwendung **Dr.Web Antivirus** auf und wählen Sie den Punkt **Einstellungen**.
  2. Auf dem Bildschirm **Dr.Web – Einstellungen** im Bereich **Modus** müssen Sie das Kontrollkästchen **Dr.Web Agent** aktivieren.
  3. Alle Einstellungen für die Verbindung mit dem **Server**, wie etwa IP-Adresse und Parameter für die Autorisierung am **Server**, werden automatisch aus der Konfigurationsdatei `install.cfg` übernommen.

  Um die Datei zu verwenden, speichern Sie diese in einem beliebigen SD-Karte-Verzeichnis der obersten Ebene ab. Wenn die Datei auf dem mobile Endgerät vorhanden ist, werden alle notwendigen Verbindungseinstellungen in die entsprechenden Felder automatisch eingegeben.

  4. Klicken Sie auf **Verbindung herstellen**.

- **Workstations unter Mac OS X**

  1. Im Menü des Programms **Dr.Web Antivirus** müssen Sie auf **Einstellungen** klicken und dann **Modus** wählen.
  2. Aktivieren Sie dann das Kontrollkästchen **Zentralschutz aktivieren**.
  3. Alle Einstellungen für die Verbindung mit dem **Server**, wie etwa IP-Adresse und Parameter für die Autorisierung am **Server**, werden automatisch aus der Konfigurationsdatei `install.cfg` übernommen.

  So nutzen Sie die Datei

  a) Klicken Sie im **Lizenz-Manager** auf den Link **Weitere Typen der Aktivierung**.

  b) Ziehen Sie die Konfigurationsdatei ins geöffnete Fenster oder klicken Sie auf den gestrichelten Rahmen, um das Dialogfeld für die Dateiauswahl zu öffnen.

  Nachdem die Datei ausgewählt wurde, werden alle notwendigen Verbindungseinstellungen in die entsprechenden Felder automatisch eingegeben.

- **Workstations unter Linux-artigen Betriebssystemen**

  1. Öffnen Sie den **Lizenz-Manager** und klicken Sie auf **Lizenz aktivieren**, um mit der Registrierung zu beginnen.
  2. Wählen Sie**Weitere Typen der Aktivierung**.
  3. Geben Sie im geöffneten Feld den Pfad zur Konfigurationsdatei an, welche alle notwendigen Verbindungs- und Autorisierungseinstellungen enthält.

2.3.2.2. Dr.Web Agent mithilfe des Installationsprogramms installieren

Das Installationsprogramm des **Agents** unterscheidet sich vom Installationspaket dadurch, dass es über keine Parameter für die Verbindung mit dem **Server** und die Autorisierung der Workstation am **Server** verfügt.

Installationsprogramme für den **Dr.Web Agent** finden Sie auf der Installationsseite des **Dr.Web Sicherheitscenters**.

Um Installationsprogramme für Nicht-Windows-Betriebssysteme und eine vollständige Distribution des Installationsprogramms für Windows-Betriebssysteme zu erhalten, müssen Sie auch die zusätzliche Distribution (extra) des **Dr.Web Servers** installieren.

Dr.Web Agent auf Workstations unter Android, Linux, Mac OS X lokal installieren

Für Workstations unter Android, Linux, Mac OS X ist das Installationsprogramm für den **Dr.Web Agent** verfügbar, das dem Installationsprogramm der eigenständigen Version ähnlich ist.

Die lokale Installation vom **Dr.Web Agent** wird im **Benutzerhandbuch** für das jeweilige Betriebssystem detailliert beschrieben.

Wenn Sie einen **Dr.Web Agent** mithilfe des Installationsprogramms ohne Konfigurationsdatei installieren, müssen Sie auf der Workstation die Adresse des **Servers** manuell angeben, damit die Workstation eine Verbindung mit ihm herstellen kann.

Sie können die Authentifizierungsparameter entweder manuell festlegen oder überhaupt nicht festlegen. Dabei kann die Verbindung mit dem **Server** wie folgt erfolgen:

Variante	Authentifizierungsparameter
Manuell	Es erfolgt ein Autorisierungsversuch anhand angegebener Authentifizierungsparameter.
Nicht festlegen	Das Verfahren zur Autorisierung am **Server** hängt von den Einstellungen des **Servers** ab, die zum Herstellen einer Verbindung mit neuen Workstations verwendet werden (mehr dazu finden Sie im **Administratorhandbuch** unter Verbindungsrichtlinie für Workstations).

Um Authentifizierungsparameter manuell festzulegen, müssen Sie zuerst im **Verwaltungscenter** ein neues Workstation-Konto erstellen. Dabei wird ein Installationspaket verfügbar sein, das eine Konfigurationsdatei mit Verbindungs- und Autorisierungseinstellungen beinhaltet. Wir empfehlen Ihnen, statt eines Installationsprogramms dieses Installationspaket zu verwenden.

Dr.Web Agent auf Workstations unter Windows lokal installieren

Zur Verfügung stehen die folgenden Typen des Installationsprogramms des **Dr.Web Agents**:

- *Netzwerk-Installer* `drwinst.exe` sorgt nur für die Installation des **Agents**. Nachdem eine Verbindung mit dem **Server** hergestellt ist, lädt der **Agent** entsprechende Komponenten des Antivirenpakets herunter und dann installiert sie.
- *Vollversion des Installationsprogramms* `drweb-esuite-agent-full-10.00.0-`*<Buildversion>*`-windows.exe` sorgt für die gleichzeitige Installation des **Agents** und Installationspakets.

Wenn Sie beim Installieren diese Installationsprogramme verwenden, können Sie die Verbindungs- und Autorisierungseinstellungen des **Servers** überhaupt nicht festlegen oder manuell festlegen.

Um Authentifizierungsparameter manuell festzulegen, müssen Sie zuerst im **Verwaltungscenter** ein neues Workstation-Konto erstellen. Dabei wird ein Installationspaket verfügbar sein. Falls keine explizite Notwendigkeit zur Installation mithilfe des Netzwerk-Installers bzw. der Vollversion des Installationsprogramms besteht, empfehlen wir Ihnen, statt eines Installationsprogramms ein Installationspaket zu verwenden.

Die Verbindung mit dem **Server** kann wie folgt erfolgen:

Variante	Server-Adresse	Authentifizierungsparameter
Manuell	Workstation greift direkt auf den festgelegten **Server** zu.	Es erfolgt ein Autorisierungsversuch anhand angegebener Authentifizierungsparameter.
Nicht festlegen	**Agent** sucht im Netzwerk nach dem **Server** mithilfe des *Server-Suchdienstes*. Es wird versucht, eine Verbindung mit dem ersten gefundenen **Server** herzustellen.	Das Verfahren zur Autorisierung am **Server** hängt von den Einstellungen des **Servers** ab, die zum Herstellen einer Verbindung mit neuen Workstations verwendet werden (mehr dazu finden Sie im **Administratorhandbuch** unter Verbindungsrichtlinie für Workstations).

Im **Benutzerhandbuch** für Windows wird die Vorgehensweise bei der Installation des **Dr.Web Agents** sowohl mithilfe der Vollversion des Installationsprogramms als auch mithilfe des Netzwerk-Installers ausführlich beschrieben.

Da die Installation mithilfe des Netzwerk-Installers meist komplizierter ist, sollte sie vom Administrator des Antivirus-Netzwerks durchgeführt werden.

Dr.Web Agent auf Workstations unter Windows mithilfe des Netzwerk-Installers lokal installieren

Der Netzwerk-Installer des **Agents** `drwinst.exe` ist nur für die Installation des **Agents** auf Workstations unter Windows geeignet.

Wenn der Netzwerk-Installer im normalen Installationsmodus (ohne den Schalter `/instMode remove`) auf der Workstation ausgeführt wird, auf der ein Agent bereits installiert wurde, werden keine Aktionen durchgeführt. Der Netzwerk-Installer wird beendet, und ein Fenster mit der Liste möglicher Schalter wird angezeigt.

Die Installation mithilfe des Netzwerk-Installers kann in zwei Modi durchgeführt werden:

1. *Im Hintergrundmodus* – dieser wird gestartet, wenn Sie den Schalter des Hintergrundmodus eingegeben haben.
2. *Im Grafikmodus* – dieser Modus startet standardmäßig, wenn Sie den Schalter des Hintergrundmodus nicht eingegeben haben.

Mithilfe des Netzwerk-Installers können Sie den **Dr.Web Agent** über das **Verwaltungscenter** (mehr dazu finden Sie unter Dr.Web Agent remote installieren) installieren.

So installieren Sie Dr.Web Agent im Hintergrundmodus des Netzwerk-Installers

1. Öffnen Sie auf dem Rechner, auf dem die Antivirensoftware installiert werden soll, das Installationsverzeichnis des **Agents** (bei der Installation des **Servers** ist das Unterverzeichnis `Installer` des Installationsverzeichnisses des **Servers**, es kann später verschoben werden), oder laden Sie auf der Installationsseite vom **Verwaltungscenter** die ausführbare Datei des Installers `drwinst.exe` und den öffentlichen Schlüssel `drwcsd.pub` herunter. Starten Sie dann die Datei `drwinst.exe` mit dem Schalter für den Hintergrundmodus `/silent yes`.

   Standardmäßig verwendet die gestartete Datei `drwinst.exe`, die keine Einstellungen zum Herstellen einer Verbindung mit dem **Server** beinhaltet, den Modus **Multicast**, bei dem das Netzwerk nach aktiven **Dr.Web Servern** durchsucht wird. Werden solche gefunden, wird es versucht, den **Agent** vom ersten im Netzwerk gefundenen **Server** zu installieren.

Bei der Verwendung des **Multicast**-Modus zum Suchen nach aktiven **Servern**, wird der **Agent** vom ersten gefundenen **Server** installiert. Wenn der vorhandene öffentliche Schlüssel dabei dem Schlüssel des **Servers** nicht entspricht, wird die Installation fehlschlagen. In diesem Fall geben Sie beim Starten des Netzwerk-Installers explizit die Adresse des **Servers** an (s. unten).

Die Datei `drwinst.exe` kann auch mit zusätzlichen Befehlszeilenoptionen gestartet werden:

- Wenn der **Multicast**-Modus nicht verwendet wird, empfehlen wir Ihnen, bei der Installation des **Agents** explizit den (vorher beim DNS-Dienst registrierten) Namen des **Servers** anzugeben:

```
drwinst /silent yes /server <Server_DNS_Name>
```

Dadurch wird das Konfigurieren des Antivirus-Netzwerks vereinfacht, das bei der erneuten Installation des **Dr.Web Servers** auf einem anderen Rechner unvermeidlich ist.

- Sie können auch die Adresse des **Servers** explizit wie folgt angeben:

```
drwinst /silent yes /server 192.168.1.3
```

- Mithilfe des Schalters `/regagent yes` kann der **Agent** bei der Installation in der Liste der installierten Software registriert werden.

Die vollständige Liste mit den Optionen des **Netzwerk-Installers** finden Sie im Dokument **Anhänge** im Anhang H2. Netzwerk-Installer.

2. Sobald der Netzwerk-Installer fertig ist, wird die Software des **Agents** (nicht das Antivirenpaket) installiert.
3. Nachdem die Workstation auf dem **Server** registriert ist (falls der **Server** so eingestellt ist), wird das Antivirenpaket automatisch installiert.
4. Starten Sie auf Anforderung des **Agents** den Rechner neu.

So installieren Sie Dr.Web Agent im Grafikmodus des Netzwerk-Installers

Öffnen Sie auf dem Rechner, auf dem die Antivirensoftware installiert werden soll, das Installationsverzeichnis des **Agents** (bei der Installation des **Servers** ist das Unterverzeichnis `Installer` des Installationsverzeichnisses des **Servers**, es kann später verschoben werden), oder laden Sie auf der Installationsseite vom **Verwaltungscenter** die ausführbare Datei des Installers `drwinst.exe` und den öffentlichen Schlüssel `drwcsd.pub` herunter. Starten Sie dann die Datei `drwinst.exe`.

Es öffnet sich das Fenster des Netzwerk-Installers vom **Dr.Web Agent**. Nächste Schritte bei der Installation des **Agents** im Grafikmodus sind den Schritten bei der Installation mithilfe des Installationspakets ähnlich. Sie müssen aber keine Einstellungen für die Verbindung mit dem **Server** angeben, falls sie in entsprechenden Befehlszeilenparametern nicht festgelegt wurden.

Informationen zur Installation vom **Agent** auf Workstations finden Sie im Dokument **Dr.Web Agent® für Windows. Benutzerhandbuch**.

2.3.3. Dr.Web Agent unter Windows® remote installieren

Dr.Web Enterprise Security Suite bietet Ihnen die Möglichkeit, nach Rechnern zu suchen, auf denen die **Dr.Web Enterprise Security Suite** noch nicht installiert wurde. Eventuell können Sie diese remote installieren.

Die Remote-Installation kann über zwei Wege erfolgen:

- Über das Verwaltungscenter.
- Über Active Directory, sofern dieser Dienst im zu schützenden lokalen Netzwerk verwendet wird.

Die Remote-Installation von **Dr.Web Agents** kann nur auf Workstations unter Windows (außer Starter/Home-Editionen) erfolgen (weitere Installationen finden Sie im Dokument **Anhänge** unter Anhang A. Vollständige Liste unterstützter Betriebssysteme).

Die Remote-Installation von **Dr.Web Agents** kann über das **Verwaltungscenter** gestartet werden, das auf einem Rechner unter Windows läuft (weitere Informationen finden Sie im Dokument **Anhänge** unter Anhang A. Vollständige Liste unterstützter Betriebssysteme).

Sie benötigen Administratorrechte an den Workstations, auf denen Sie **Dr.Web Agents** installieren möchten.

Zur Remote-Installation über das **Verwaltungscenter**, sofern die Workstations in einer Domäne organisiert sind, und bei der Installation ein Domänenkonto des Administrators verwendet wird, muss Datei- und Druckerfreigabe aktiviert werden (entsprechende Einstellungen für das jeweilige Windows-Betriebssystem finden Sie in der Tabelle unten).

Wenn die Workstations in keiner Domäne organisiert sind, oder bei der Installation ein lokales Konto verwendet wird, sollten Workstations unter einigen Versionen von Windows zusätzlich konfiguriert werden.

Zusätzliche Einstellungen bei der Remote-Installation auf einer Workstation außerhalb der Domäne bzw. bei Verwendung eines lokalen Kontos

Durch angegebene Einstellungen kann die Sicherheit auf dem Remote-Rechner beeinträchtigt werden. Bevor Sie eine Änderung am System vornehmen werden, empfehlen wir Ihnen dringend, sich mit diesen Einstellungen vertraut zu machen, bzw. auf die Remote-Installation zu verzichten und den **Agent** manuell zu installieren.

Nachdem die Workstation entsprechend angepasst ist, setzen Sie die geänderten Einstellungen auf die Windows-Standardeinstellungen zurück, damit die Basissicherheitsrichtlinie des Systems nicht verletzt wird.

Bei der Remote-Installation des **Agents** auf einer Workstation außerhalb der Domäne und/oder bei Verwendung eines lokalen Kontos müssen Sie auf dem Rechner, auf dem der **Agent** remote installiert wird, die folgenden Aktionen durchzuführen:

Betriebssystem	Einstellung	
Windows XP	Zugriff auf freigegebene Dateien einstellen	Standardansicht: **Start → Einstellungen → Systemsteuerung → Darstellung und Designs → Ordneroptionen** → Registerkarte **Ansicht** → deaktivieren Sie das Kontrollkästchen **Einfache Dateifreigabe verwenden (empfohlen).**
		Klassische Ansicht: **Start → Einstellungen → Systemsteuerung → Ordneroptionen** → Registerkarte **Ansicht** → deaktivieren Sie das Kontrollkästchen **Einfache Dateifreigabe verwenden (empfohlen).**

Betriebssystem	Einstellung	
	Einstellungen zur Authentifizierung von Netzwerkanmeldungen konfigurieren	Standardansicht: **Start→ Einstellungen → Systemsteuerung → Leistung und Wartung → Verwaltung → Lokale Sicherheitsrichtlinie → Sicherheitseinstellungen → Lokale Richtlinien → Sicherheitsoptionen → Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten → Klassisch – lokale Benutzer authentifizieren sich als sie selbst**.
		Klassische Ansicht: **Start→ Einstellungen → Systemsteuerung → Verwaltung → Lokale Sicherheitsrichtlinie → Sicherheitseinstellungen → Lokale Richtlinien → Sicherheitsoptionen → Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten → Klassisch – lokale Benutzer authentifizieren sich als sie selbst**.
	Bevor Sie mit der Remote-Installation beginnen, deaktivieren Sie die Windows-Firewall.	
Windows Server 2003	Bevor Sie mit der Remote-Installation beginnen, deaktivieren Sie die Windows-Firewall.	
Windows Vista Windows Server 2008	Freigabe von Dateien einschalten	Standardansicht: **Start→ Einstellungen → Systemsteuerung → Netzwerk und Internet → Netzwerk- und Freigabecenter → Freigabe und Erkennung → Freigabe von Dateien → An**.
		Klassische Ansicht: **Start→ Einstellungen → Systemsteuerung → Netzwerk- und Freigabecenter → Freigabe und Erkennung → Freigabe von Dateien → An**.
	Einstellungen zur Authentifizierung von Netzwerkanmeldungen konfigurieren	Standardansicht: **Start→ Einstellungen → Systemsteuerung → System und Wartung → Verwaltung → Lokale Sicherheitsrichtlinie → Sicherheitseinstellungen → Lokale Richtlinien → Sicherheitsoptionen → Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten → Klassisch – lokale Benutzer authentifizieren sich als sie selbst**.
		Klassische Ansicht: **Start→ Systemsteuerung → Verwaltung → Lokale Sicherheitsrichtlinie → Sicherheitseinstellungen → Lokale Richtlinien → Sicherheitsoptionen → Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten → Klassisch – lokale Benutzer authentifizieren sich als sie selbst**.
	Erstellen Sie den Schlüssel **LocalAccountTokenFilterPolicy**:	

Betriebssystem	Einstellung	
	a) Öffnen Sie im Registrierungs-Editor den Pfad **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**. Wenn der Eintrag **LocalAccountTokenFilterPolicy** nicht vorhanden ist, wählen Sie im Menü **Bearbeiten** den Punkt **Neu** und dann **DWORD-Wert**. Geben Sie als Schlüsselnamen **LocalAccountTokenFilterPolicy** und drücken Sie die EINGABETASTE. b) Wählen Sie im Kontextmenü des Schlüssels **LocalAccountTokenFilterPolicy** **Ändern**. c) Geben Sie **1** ins Feld **Wert** ein und klicken Sie auf **OK**. Ein Neustart ist nicht erforderlich.	
Windows 7 Windows Server 2008 R2	Datei- und Druckerfreigabe aktivieren	Standardansicht: **Start→ Systemsteuerung → Netzwerk und Internet → Netzwerk- und Freigabecenter → Erweiterte Freigabeeinstellungen ändern → Datei- und Druckerfreigabe → Datei- und Druckerfreigabe aktivieren.**
		Klassische Ansicht: **Start→ Systemsteuerung → Netzwerk- und Freigabecenter → Erweiterte Freigabeeinstellungen ändern → Datei- und Druckerfreigabe → Datei- und Druckerfreigabe aktivieren.**
	Einstellungen zur Authentifizierung von Netzwerkanmeldungen konfigurieren	Standardansicht: **Start → Systemsteuerung → System und Sicherheit → Verwaltung → Lokale Sicherheitsrichtlinie → Sicherheitseinstellungen → Lokale Richtlinien → Sicherheitsoptionen → Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten → Klassisch – lokale Benutzer authentifizieren sich als sie selbst**.
		Klassische Ansicht: **Start→ Systemsteuerung → Verwaltung → Lokale Sicherheitsrichtlinie → Sicherheitseinstellungen → Lokale Richtlinien → Sicherheitsoptionen → Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten → Klassisch – lokale Benutzer authentifizieren sich als sie selbst**.
	Erstellen Sie den Schlüssel **LocalAccountTokenFilterPolicy**: a) Öffnen Sie im Registrierungs-Editor den Pfad **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**. Wenn der Eintrag **LocalAccountTokenFilterPolicy** nicht vorhanden ist, wählen Sie im Menü **Bearbeiten** den Punkt **Neu** und dann **DWORD-Wert**. Geben Sie als Schlüsselnamen **LocalAccountTokenFilterPolicy** und drücken Sie die EINGABETASTE. b) Wählen Sie im Kontextmenü des Schlüssels **LocalAccountTokenFilterPolicy** **Ändern**. c) Geben Sie **1** ins Feld **Wert** ein und klicken Sie auf **OK**. Ein Neustart ist nicht erforderlich.	
Windows 8 Windows 8.1	Datei- und Druckerfreigabe aktivieren	Standardansicht:

Betriebssystem	Einstellung	
Windows Server 2012 Windows Server 2012 R2		**Einstellungen → Systemsteuerung → Netzwerk und Internet → Netzwerk- und Freigabecenter → Erweiterte Freigabeeinstellungen ändern → Datei- und Druckerfreigabe → Datei- und Druckerfreigabe aktivieren.**
		Klassische Ansicht: **Einstellungen→ Systemsteuerung → Netzwerk- und Freigabecenter → Erweiterte Freigabeeinstellungen ändern → Datei- und Druckerfreigabe → Datei- und Druckerfreigabe aktivieren.**
	Einstellungen zur Authentifizierung von Netzwerkanmeldungen konfigurieren	Standardansicht: **Einstellungen→ Systemsteuerung → System und Sicherheit → Verwaltung → Lokale Sicherheitsrichtlinie → Sicherheitseinstellungen → Lokale Richtlinien → Sicherheitsoptionen → Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten → Klassisch – lokale Benutzer authentifizieren sich als sie selbst**.
		Klassische Ansicht: **Einstellungen→ Systemsteuerung → Verwaltung → Lokale Sicherheitsrichtlinie → Sicherheitseinstellungen → Lokale Richtlinien → Sicherheitsoptionen → Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten → Klassisch – lokale Benutzer authentifizieren sich als sie selbst**.
	Erstellen Sie den Schlüssel **LocalAccountTokenFilterPolicy**: a) Öffnen Sie im Registrierungs-Editor den Pfad **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**. Wenn der Eintrag **LocalAccountTokenFilterPolicy** nicht vorhanden ist, wählen Sie im Menü **Bearbeiten** den Punkt **Neu** und dann **DWORD-Wert**. Geben Sie als Schlüsselnamen **LocalAccountTokenFilterPolicy** und drücken Sie die EINGABETASTE. b) Wählen Sie im Kontextmenü des Schlüssels **LocalAccountTokenFilterPolicy Ändern**. c) Geben Sie **1** ins Feld **Wert** ein und klicken Sie auf **OK**. Ein Neustart ist nicht erforderlich.	

Wenn für das Konto auf der Workstation ein leeres Password definiert wurde, setzen Sie außer Kraft die für Null-Kennwörter geltenden Beschränkungen mithilfe einer Richtlinie: **Systemsteuerung → Verwaltung → Lokale Sicherheitsrichtlinie → Sicherheitseinstellungen → Lokale Richtlinien → Sicherheitsoptionen → Konten: Lokale Kontenverwendung von leeren Kennwörtern auf Konsolenanmeldung beschränken → Deaktiviert**.

Die Installationsprogrammdatei vom **Agent** `drwinst.exe` sowie der öffentliche Schlüssel `drwcsd.pub` müssen auf einer gemeinsam genutzten Ressource abgespeichert werden.

2.3.3.1. Dr.Web Agent über das Dr.Web Verwaltungscenter installieren

Die Remote-Installation der Agents auf Workstations kann auf folgende Arten geschehen:

1. Über Netzwerk-Scanner installieren

   Bei dieser Installationsart wird es nach ungeschützten Rechnern innerhalb des Netzwerks gesucht. Wenn solche gefunden werden, können Sie **Dr.Web Agents** darauf installieren.

2. Über Netzwerk installieren

   Von dieser Installationsart profitieren Sie besonders dann, wenn Sie die Adresse der Workstation oder Gruppe von Workstations kennen, auf denen **Agents** installiert werden sollen.

3. Agent auf Workstations mit festgelegten IDs installieren

   Bei dieser Installationsart können **Agents** für ausgewählte Konten (darunter alle bereits vorhandenen neuen Konten) mit festgelegten IDs und Passwörtern für den Zugriff auf den **Server** auf Workstations oder Gruppen von Workstations installiert werden.

Damit der **Netzwerk-Scanner** und der **Netzwerk-Installer** im Windows Internet Explorer voll funktionsfähig bleiben, muss die IP-Adresse und/oder der DNS-Name des Rechners, auf dem **Dr.Web Server** installiert ist, zur Liste der vertrauenswürdigen Webseiten des Browsers, in dem Sie das **Verwaltungscenter** zur Remote-Installation öffnen, hinzugefügt werden.

Installation mithilfe des Netzwerk-Scanners

In der hierarchischen Liste des Antivirus-Netzwerks vom **Verwaltungscenter** werden Rechner angezeigt, die dem Antivirus-Netzwerk bereits angehören. In **Dr.Web Enterprise Security Suite** können Sie aber auch nach Rechnern suchen, die durch die Antivirensoftware von **Dr.Web Enterprise Security Suite** noch nicht geschützt sind. Falls Sie solche gefunden haben, können Sie darauf entsprechende Antivirenkomponenten remote installieren.

Um die Software vom **Agent** auf Workstations schnell zu installieren, können Sie den **Netzwerk-Scanner** (mehr dazu finden Sie im **Administratorhandbuch** unter Netzwerk-Scanner) verwenden. Der Netzwerk-Scanner findet Rechner nach ihre IP-Adressen.

So installieren Sie Agents mithilfe des Netzwerk-Scanners

1. Öffnen Sie den **Netzwerk-Scanner**. Wählen Sie dafür **Administrierung** im Hauptmenü vom **Verwaltungscenter**. Wählen Sie im geöffneten Fenster den Menüpunkt **Netzwerk-Scanner**. Es öffnet sich das gleichnamige Fenster ohne Workstations.
2. Aktivieren Sie das Kontrollkästchen **Suche nach IP-Adressen**, um im Netzwerk nach Workstations innerhalb des angegebenen IP-Adressbereiches zu suchen. Geben Sie in das Eingabefeld **Netzwerke** den gewünschten IP-Adressbereich wie folgt ein:
   - Durch einen Bindestrich getrennt (z. B. `10.4.0.1-10.4.0.10`).
   - Durch ein Komma und Leerzeichen getrennt (z. B. `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`).
   - Durch Angabe eines Netzwerkpräfixes (z.B. `10.4.0.0/24`).
3. Aktivieren Sie unter Windows das Kontrollkästchen **In Active Directory suchen**, um nach Workstations in der Active Directory-Domäne zu suchen. Legen Sie die folgenden Parameter fest:
   - **Domänen** – ist die Liste der Domänen, in denen es nach Workstations gesucht wird. Verwenden Sie das Komma-Zeichen, um mehrere Domänen voneinander zu trennen.
   - **Active Directory-Controller** – ist der Active Directory Controller, z.B. dc.example.com.

Um nach Workstations in einer Active Directory-Domäne über den **Netzwerk-Scanner** zu suchen, muss der Webbrowser, in dem das **Verwaltungscenter** geöffnet ist, unter dem Domänenbenutzerkonto ausgeführt werden, das über die Berechtigung zur Suche nach Active Directory-Objekten verfügt.

Eine nähere Beschreibung der erweiterten Einstellungen finden Sie im **Administratorhandbuch** unter Netzwerk-Scanner.

4. Klicken Sie auf **Scannen**. Im Fenster wird ein Verzeichnis (eine hierarchische Liste) aller Rechner angezeigt, auf denen die Antivirensoftware bereits installiert bzw. noch nicht installiert ist.
5. Erweitern Sie die Elemente des Verzeichnisses, die den Arbeitsgruppen (Domänen) entsprechen. Alle Elemente des Verzeichnisses, die den Arbeitsgruppen und einzelnen Workstations entsprechen, werden durch unterschiedliche Symbole markiert. Ihre jeweilige Bedeutung finden Sie in der Tabelle unten.

Tabelle2-1: Mögliche Symbole

Symbol	Erläuterung
	Arbeitsgruppen
	Arbeitsgruppen, zu denen u. a. die Rechner gehören, auf denen **Dr.Web Enterprise Security Suite** installiert werden kann.
	Sonstige Gruppen, zu denen Rechner mit bereits installierter Antivirensoftware bzw. im Netzwerk nicht verfügbare Rechner gehören.
	Workstations
	Die gefundene Workstation ist in der Datenbank registriert und aktiv (aktive Workstations mit der installierten Antivirensoftware).
	Die gefundene Workstation ist in der Datenbank, in der Tabelle der gelöschten Workstations registriert.
	Die gefundene Workstation ist in der Datenbank nicht registriert (auf dem Rechner ist keine Antivirensoftware vorhanden).
	Die gefundene Workstation ist in der Datenbank nicht registriert (die Workstation ist mit einem anderen **Server** verbunden).
	Die gefundene Workstation ist in der Datenbank zwar registriert, ist aber nicht aktiv, und der Port ist geschlossen.

Die Verzeichniselemente, die den Workstations mit dem Symbol oder entsprechen, können erweitert werden. Dabei können Sie auch die darauf installierten Komponenten einsehen.

6. Wählen Sie im Fenster des **Netzwerk-Scanners** einen ungeschützten Rechner (zur Mehrfachauswahl verwenden Sie die STRG- bzw. UMSCHALTTASTE).
7. Klicken Sie in der Symbolleiste die Schaltfläche **Dr.Web Agent installieren** an.
8. Es öffnet sich das Fenster **Installation im Netzwerk**, in dem Sie die Aufgabe zur Installation des **Agents** erstellen können.
9. Im Feld **Namen der PCs** wird die IP-Adresse des Rechners (der Rechner) angegeben, auf dem (denen) die Antivirensoftware installiert werden soll.
   - Bei der Installation auf den Workstations, die über den **Netzwerk-Scanner** gefunden wurden, wird im Feld **Rechner** bereits die Adresse der Workstation bzw. mehrerer Workstations angegeben, auf denen die Antivirensoftware installiert wird.
   - Sollte es nicht der Fall sein, müssen Sie die Adresse der Workstation bzw. Workstations manuell angeben. Wenn Sie die Software des **Agents** gleichzeitig auf mehreren Rechnern installieren wollen, können Sie mehrere IP-Adressen der Rechner wie folgt angeben:
     - Durch einen Bindestrich getrennt (z. B. `10.4.0.1-10.4.0.10`).
     - Durch ein Komma und Leerzeichen getrennt (z. B. `10.4.0.1-10.4.0.10, 10.4.0.35-10.4.0.90`).

- Durch Angabe eines Netzwerkpräfixes (z. B. `10.4.0.0/24`).

Anstatt der IP-Adressen können Sie auch Domänennamen der Rechner angeben.

10. Standardmäßig wird die Software des **Agents** im Verzeichnis `%ProgramFiles%\DrWeb` installiert. Geben Sie gegebenenfalls im Feld **Installationsverzeichnis** einen anderen Pfad an.

    Geben Sie möglichst immer den vollständigen Pfad zum Installationsverzeichnis an, um die Installation erfolgreich durchzuführen. Bei der Pfadangabe können Sie auch Umgebungsvariablen verwenden.

11. Im Feld **Server** wird standardmäßig die IP-Adresse bzw. der DNS-Name vom **Dr.Web Server** angezeigt, mit dem das **Verwaltungscenter** verbunden ist. Bei Bedarf können Sie in diesem Feld die Adresse des **Servers** angeben, den zum Installieren der Antivirensoftware verwendet wird. Um mehrere **Server** einzugeben, verwenden Sie als Trennzeichen „;“ oder „; “.
12. Geben Sie im Feld **Öffentlicher Schlüssel** den Pfad des öffentlichen Schlüssels an.
13. Geben Sie im Feld **Ausführbare Installationsdatei** den Pfad zum Netzwerk-Installer an. Ändern Sie bei Bedarf die vorhandenen Werte und legen Sie zusätzlich andere Parameter fest.

Pfade zum öffentlichen Schlüssel und zur ausführbaren Datei müssen im Format von Netzwerkadressen angegeben werden.

14. Wählen Sie in der Dropdown-Liste **Sprache** die Sprache der Benutzeroberfläche vom **Dr.Web Antivirus**, der auf den Workstations installiert wird.
15. Geben Sie bei Bedarf im Feld **Erweiterte Parameter** Befehlszeilenoptionen zum Starten des Netzwerk-Installers (mehr dazu finden Sie im Dokument **Anhänge** im H2. Netzwerk-Installer) an.
16. Definieren Sie im Feld **Installations-Timeout (Sek)** die maximale Wartezeit in Sekunden bis zum Ende der Installation des**Agents**. Zulässige Werte: 1-600. Standardmäßig ist dieser Wert auf 180 Sekunden gesetzt. Bei einer geringen Datenübertragungsrate des Übertragungskanals zwischen dem **Server** und **Agent** empfehlen wir Ihnen, diesen Wert zu erhöhen.
17. Aktivieren Sie bei Bedarf das Kontrollkästchen **Installation in der Liste der installierten Programme registrieren**.
18. Wählen Sie im Bereich **Installieren** die Komponenten des Antivirenpakets aus, die auf der Workstation installiert werden sollen.
19. Legen Sie im Bereich **Komprimierung** und **Verschlüsselung** die Parameter zur Komprimierung des Datenverkehrs bei der Installation fest.
20. Geben Sie im Bereich **Autorisierung auf dem entfernt gelegenen Rechner** entsprechende Autorisierungsdaten für den Zugriff auf den Remote-Rechner an.

    Sie können mehrere Administrator-Konten festlegen. Um ein neues Konto hinzuzufügen, klicken Sie auf und geben in die entsprechenden Felder alle notwendigen Autorisierungsdaten ein. Diese Vorgehensweise gilt für jedes neue Konto.

    Bei der Installation des **Agents** wird das oberste Konto in der Liste verwendet. Wenn die Installation unter diesem Konto fehlgeschlagen ist, wird das nächste usw. Konto verwendet.

21. Nachdem Sie alle notwendigen Parameter festgelegt haben, klicken Sie auf **Installieren**.

Damit die Installation der Antivirensoftware gestartet werden kann, wird der integrierte Dienst verwendet.

22. **Dr.Web Agent** wird auf den angegebenen Workstations installiert. Nachdem die Workstation auf dem **Server** bestätigt wird (falls der **Dr.Web Server** so eingestellt ist, mehr dazu finden Sie im **Administratorhandbuch** unter Verbindungsrichtlinie für Workstations), wird das Antivirenpaket automatisch installiert.

23. Starten Sie auf Anforderung des **Agents** den Rechner neu.

Installation über Netzwerk

Wenn Sie das Antivirus-Netzwerk im Wesentlichen bereits eingerichtet haben und nun die Software vom **Agent** auf bestimmten Rechnern installieren wollen, empfehlen wir Ihnen, die **Installation über Netzwerk** zu verwenden.

So installieren Sie den Agent über Netzwerk

1. Wählen Sie im Hauptmenü den Punkt **Administrierung** und dann den Menüpunkt **Installation im Netzwerk**.
2. Gehen Sie weiter so wie oben unter **8-22** beschrieben vor.

Installation für Konten mit festgelegten IDs

So können Sie Agents für Konten mit ausgewählten IDs remote installieren

a) Beim Erstellen eines neuen Workstation-Kontos:
   1. Erstellen Sie ein neues Konto bzw. mehrere Konten für Workstations (mehr dazu finden Sie unter Neues Konto erstellen).
   2. Sobald das neue Konto erstellt wurde, öffnet sich im rechten Teil des Hauptfensters das Panel mit der Überschrift **Workstation erstellen**. Klicken Sie auf **Installieren**.
   3. Es öffnet sich das Fenster des **Netzwerk-Scanners**.
   4. Gehen Sie weiter so wie oben unter **2-22** beschrieben vor.
   5. Nachdem die Installation abgeschlossen ist, stellen Sie sicher, dass die Symbole der Workstations in der hierarchischen Liste entsprechend aktualisiert wurden.

b) Bei der Verwendung eines bestehenden Workstation-Kontos:
   1. Wählen Sie in der hierarchischen Liste des Antivirus-Netzwerks eine neue Workstation bzw. eine Gruppe von Workstations, auf denen noch keine **Agents** installiert wurden, oder wählen Sie die Gruppe **New** (bei der Installation für alle vorhandenen neuen Konten) aus.
   2. Klicken Sie in der Symbolleiste auf **Dr.Web Agent installieren**.
   3. Es öffnet sich das Fenster des **Netzwerk-Scanners**.
   4. Gehen Sie weiter so wie oben unter **2-22** beschrieben vor.
   5. Nachdem die Installation abgeschlossen ist, stellen Sie sicher, dass die Symbole der Workstations in der hierarchischen Liste entsprechend aktualisiert wurden.

Der **Agent** kann auf der Workstation mit ausgewählten IDs auch vom Gruppenadministrator installiert werden.

Wenn Fehler bei der Remote-Installation auftreten, lesen Sie den ansprechenden Abschnitt im Dokument **Anhänge** Probleme bei der Remote-Installation beheben.

2.3.3.2. Dr.Web Agent über Active Directory installieren

Wenn der **Active Directory**-Dienst im geschützten lokalen Netzwerk verwendet wird, können Sie **Dr.Web Agents** auf Workstations remote installieren.

Die Installation vom **Agent** über Active Directory ist auch unter Verwendung des verteilten Dateisystems DFS möglich (s. **Anhänge** unter DFS bei der Installation des Agents über Active Directory verwenden).

Agent installieren

So installieren Sie einen Agent über Active Directory

1. Laden Sie unter http://download.drweb.com/esuite/ das Installationsprogramm des **Dr.Web Agents** für Netzwerke mit **Active Directory** herunter.
2. Führen Sie auf dem Server des lokalen Netzwerks, der den **Active Directory**-Dienst unterstützt, die administrative Installation des **Dr.Web Agents** durch. Die Installation kann sowohl über die Befehlszeile **(A)** als auch über die grafische Oberfläche des Installationsprogramms **(B)** erfolgen.

Bei der Aktualisierung des **Servers** ist es nicht erforderlich, das Installationsprogramm des **Dr.Web Agents** für Netzwerke mit Active Directory mitzuaktualisieren. Sobald die Software des **Servers** aktualisiert wurde, werden die **Agents** und Antivirensoftware auf den Workstations automatisch nach der Installation aktualisiert.

(A) Parameter für die Installation des Dr.Web Agents im Befehlszeilenmodus konfigurieren

Führen Sie den folgenden Befehl mit allen erforderlichen Parametern und mit der obligatorischen Option zur Deaktivierung der graphischen Oberfläche `/qn` aus:

`msiexec /a` *<Paketname>*`.msi /qn [`*<Parameter>*`]`

Der Schalter `/a` führt die administrative Installationsoption aus.

Paketname

Der Name des Installationspakets des **Dr.Web Agents** für Netzwerke mit **Active Directory** hat in der Regel das folgende Format:

`drweb-esuite-agent-activedirectory-`*<Version>*`-`*<Releasedatum>*`.msi`.

Parameter

`/qn` – Befehlszeilenoption zur Deaktivierung der grafischen Oberfläche. Wenn sie verwendet wird, müssen Sie die folgenden obligatorischen Parameter festlegen:

- `ESSERVERADDRESS=`*<DNS_Name>* – liefert die Adresse vom **Dr.Web Server**, mit dem sich der **Agent** verbinden soll. Informationen zu verfügbaren Formaten finden Sie im Dokument **Anhänge** unter Anhang E3.
- `ESSERVERPATH=`*<Pfad_Dateimname>* – liefert den vollständigen Pfad zum öffentlichen Schlüssel vom **Dr.Web Server** und den Dateinamen (standardmäßig ist das die Datei `drwcsd.pub` im Unterverzeichnis `Installer` des Installationsverzeichnisses vom **Dr.Web Server**).
- `TARGETDIR` – ist das Netzwerkverzeichnis für das Abbild vom **Agent** (dem modifizierten Installationspaket vom **Agent**), das über den Gruppenrichtlinienverwaltungs-Editor für die geplante Installation ausgewählt wird. Dieses Verzeichnis muss über Lese- und Schreibzugriff verfügen. Der Pfad zum Verzeichnis muss im Format von Netzwerkadressen angegeben werden, selbst wenn das Verzeichnis lokal verfügbar ist. Außerdem muss es die Möglichkeit bestehen, auf das Verzeichnis von Zielworkstations zuzugreifen.

Vor der administrativen Installation brauchen Sie Installationsdateien ins Zielverzeichnis für das Abbild vom **Agent** (s. den Parameter `TARGETDIR`) manuell nicht zu kopieren. Das Installationsprogramm vom **Agent** für Netzwerke mit Active Directory (*<Paketname>*`.msi`) und sonstige Dateien, die für die Installation der **Agents** notwendig sind, werden bei der administrativen Installation ins Zielverzeichnis automatisch kopiert. Wenn diese Dateien im Zielverzeichnis bereits vorhanden sind, werden alle gleichnamigen Dateien überschrieben.

Wenn Sie bei der administrativen Installation mehrere **Server** verwenden, empfehlen wir Ihnen, für jeden der **Server** verschiedene Zielverzeichnisse anzugeben.

Nach der Bereitstellung des administrativen Pakets muss sich im Verzeichnis *<Zielverzeichnis>*`\Program Files\DrWeb` nur die Datei `README.txt` befinden.

Beispiele:

```
msiexec /a ES_Agent.msi /qn ESSERVERADDRESS=servername.net ESSERVERPATH=\\win_serv
\drwcs_inst\drwcsd.pub TARGETDIR=\\comp\share
```

```
msiexec /a ES_Agent.msi /qn ESSERVERADDRESS=192.168.14.1 ESSERVERPATH="C:\Program
Files\DrWeb Server\Installer\drwcsd.pub" TARGETDIR=\\comp\share
```

Die oben genannten Parameter können auch in der grafischen Oberfläche des Installationsprogramms festgelegt werden.

Danach ist es erforderlich, die Installation des Pakets auf dem Server des lokalen Netzwerks zu konfigurieren, auf dem die Software für Active Directory Verwaltung installiert ist (s. Vorgehensweise unten).

(B) Parameter für die Installation des Dr.Web Agents im grafischen Modus konfigurieren

Vor dem Beginn der administrativen Installation müssen Sie sicherstellen, dass das Zielverzeichnis für das Abbild vom **Agent** kein Installationsprogramm des **Dr.Web Agents** für Netzwerke mit **Active Directory** beinhaltet (*<Paketname>*`.msi`).

Nach der Bereitstellung des administrativen Pakets muss sich im Verzeichnis:

<Zielverzeichnis>`\Program Files\DrWeb`

nur die Datei `README.txt` befinden.

1. Um das Installationsprogramm im grafischen Modus zu starten, führen Sie den folgenden Befehl aus:

   `msiexec /a` *<Pfad_zum_Installationsprogramm>*`\`*<Paketname>*`.msi`

2. Es öffnet sich das Fenster **InstallShield Wizard** mit Informationen zum zu installierenden Produkt. Klicken Sie die Schaltfläche **Weiter** an.

Das Installationsprogramm des **Agents** wird in der Sprache angezeigt, die in den Spracheinstellungen des Rechners als Anzeigesprache festgelegt ist.

3. Geben Sie im neuen Fenster den DNS-Namen oder die IP-Adresse vom **Dr.Web Server** (mehr dazu finden Sie im Dokument **Anhänge** unter Anhang E3) an. Geben Sie den Speicherort des öffentlichen Schlüssels des **Dr.Web Servers** (`drwcsd.pub`) an. Klicken Sie die Schaltfläche **Weiter** an.

4. Geben Sie im nächsten Fenster das Netzwerkverzeichnis an, in welches das Abbild des **Agents** kopiert werden soll. Der Pfad zum Abbild muss im Format von Netzwerkadressen angegeben werden, selbst wenn das Verzeichnis lokal verfügbar ist. Außerdem muss es die Möglichkeit bestehen, auf das Verzeichnis von Workstations aus zuzugreifen. Klicken Sie die Schaltfläche **Installieren** an.
5. Nachdem die Installation abgeschlossen ist, öffnet sich automatisch das Einstellungsfenster, in dem Sie die Installation der Pakete auf den Rechnern des Netzwerks einplanen können.

Installation des Pakets auf ausgewählten Workstations konfigurieren

1. Wählen Sie in **Systemsteuerung** (bzw. im **Start**-Menü unter Windows 2003/2008 Server, in **Start → Programme** unter Windows 2000 Server) **Verwaltung → Active Directory-Benutzer und -Computer** (im grafischen Installationsmodus vom **Agent** erscheint dieses Einstellungsfenster automatisch).
2. In der Domäne, der die Rechner angehören, auf denen **Dr.Web Agents** installiert werden sollen, müssen Sie eine neue **Organisationseinheit** erstellen und ihr einen Namen vergeben, z. B. **ESS**. Wählen Sie dafür im Kontextmenü der Domäne den Eintrag **Neu → Organisationseinheit**. Geben Sie im geöffneten Fenster den gewünschten Namen der zu erstellenden Organisationseinheit an und klicken Sie dann auf **OK**. Fügen Sie der erstellten Organisationseinheit Rechner hinzu, auf denen der **Agent** installiert werden soll.
3. Öffnen Sie das Fenster der Gruppenrichtlinienverwaltung. Gehen Sie dafür wie folgt vor:
   a) Unter Windows 2000/2003 Server: Wählen Sie im Kontextmenü der erstellten Organisationseinheit **ESS** den Eintrag **Eigenschaften**. Klicken Sie im geöffneten Fenster auf die Registerkarte **Gruppenrichtlinie**.
   b) Unter Windows 2008 Server: **Start → Verwaltung → Gruppenrichtlinienverwaltung**.
4. Legen Sie für die erstellte Organisationseinheit eine Gruppenrichtlinie fest. Gehen Sie wie folgt vor:
   a) Unter Windows 2000/2003 Server: Klicken Sie auf **Hinzufügen** und erstellen Sie eine Richtlinie mit dem Namen **ESS**. Doppelklicken Sie dann darauf.
   b) Unter Windows 2008 Server: Wählen Sie im Kontextmenü der erstellten Organisationseinheit **ESS** den Eintrag **Gruppenrichtlinienobjekt hier erstellen und verknüpfen**. Geben Sie im geöffneten Fenster den gewünschten Namen des neuen Gruppenrichtlinienobjektes und klicken Sie dann auf **OK.** Wählen Sie im Kontextmenü der neuen Gruppenrichtlinie den Eintrag **Bearbeiten**.
5. Nehmen Sie im geöffneten Fenster vom **Gruppenrichtlinienverwaltungs-Editor** entsprechende Einstellungen für die unter dem Punkt **4**erstellte Gruppenrichtlinie vor. Gehen Sie dafür wie folgt vor:
   a) Unter Windows 2000/2003 Server: Wählen Sie in der Liste den Bereich **Computerkonfiguration → Computerkonfiguration → Softwareinstallation**.
   b) Unter Windows 2008 Server: Wählen Sie in der Liste den Bereich **Computerkonfiguration → Richtlinien → Softwareeinstellungen → Softwareinstallation**.
6. Wählen Sie im Kontextmenü des Bereichs **Softwareinstallation** den Eintrag **Neu → Paket**.
7. Wählen Sie dann das Installationspaket des **Agents**. Geben Sie dafür die Adresse der gemeinsam genutzten Netzwerkressource (d. h. die des bei der administrativen Installation erstellten Abbildes des **Agents**) an. Der Pfad zum Verzeichnis mit dem Paket muss im Format von Netzwerkadressen angegeben werden, selbst wenn das Verzeichnis lokal verfügbar ist.
8. Es öffnet sich das Fenster **Software bereitstellen**. Wählen Sie hier die Option **Zugewiesen** und klicken Sie dann auf **OK**.
9. Das neue Paket wird unter dem Namen **Dr.Web Agent** im rechten Bereich des Gruppenrichtlinienverwaltungs-Editors angezeigt. Wählen Sie im Kontextmenü dieses Paketes **Eigenschaften** aus.
10. Wechseln Sie im geöffneten Fenster von Paketeigenschaften zur Registerkarte **Bereitstellung**. Klicken Sie dann auf **Erweitert**.

11. Es öffnet sich das Dialogfeld **Erweiterte Bereitstellungsoptionen**.
    - Aktivieren Sie das Kontrollkästchen **Sprache beim Bereitstellen dieses Pakets ignorieren**.
    - Wenn Sie den **Dr.Web Agent** über das konfigurierbare MSI-Paket auf den Rechnern unter 64-Bit-Betriebssystemen installieren wollen, aktivieren Sie das Kontrollkästchen **Diese 32-Bit-X86-Anwendung für Win64-Computer bereitstellen**.
12. Doppelklicken Sie auf **OK**.
13. **Dr.Web Agent** wird auf den ausgewählten Rechnern installiert, sobald sie in der Domäne registriert sind.

Richtlinien mit Rücksicht auf vorherige Installationen des Agents anwenden

Beim Zuweisen von Active Directory-basierten Richtlinien für die Installation des **Agents** muss berücksichtigt werden, dass der **Agent** auf einigen Workstations bereits installiert sein kann. In diesem Zusammenhang sind drei Varianten möglich:

1. **Auf der Workstation gibt es keinen installierten Dr.Web Agent**.

   Sobald die Richtlinien angewendet sind, wird der **Agent** wie oben beschrieben installiert.

2. **Dr.Web Agent wurde auf der Workstation bereits ohne Active Directory installiert**.

   Sobald Active Directory-basierten Richtlinien angewendet sind, bleibt der bereits installierte **Agent** auf der Workstation weiterhin erhalten.

   Obwohl der **Agent** in diesem Fall auf der Workstation installiert ist, erkennt der Active Directory-Dienst den **Agent** als nicht installiert. Jedes Mal, wenn die Workstation hochgefahren ist, tritt aus diesem Grund ein nicht vorübergehender Fehler bei der Installation des **Agents** über Active Directory auf.

   Um den **Agent** über Active Directory zu installieren, müssen Sie den bereits installierten **Agent** manuell (bzw. über das **Verwaltungscenter**) deinstallieren und Active Directory-basierten Richtlinien dieser Workstation erneut zuweisen.

3. **Dr.Web Agent wurde auf der Workstation über Active Directory installiert**.

   Gruppenrichtlinien sind bereits angewendet:

   a) Wenn der Workstation die Berechtigung für die Deinstallation des **Agents** zugewiesen wurde, wird dieser von der Workstation entfernt. Um den **Agent** über Active Directory zu installieren, müssen Sie Active Directory-basierte Richtlinien dieser Workstation erneut zuweisen.

   In diesem Fall müssen Sie die Richtlinien für die Installation des **Agents** erneut zuweisen, da der **Agent** von Active Directory als installiert erkannt wird, obwohl der **Agent** nach dem ersten Zuweisen der Richtlinien von der Workstation entfernt wurde.

   b) Wenn der Workstation keine Berechtigung für die Deinstallation des **Agents** zugewiesen wurde, bleibt die Antivirensoftware der Workstation von den Richtlinien unbeeinflusst. Um die Installation fortzusetzen, müssen Sie die Berechtigung für die Deinstallation des **Agents** (mehr dazu finden Sie im **Administratorhandbuch** unter Benutzerrechte konfigurieren) festlegen und Active Directory-basierte Richtlinien der Workstation erneut zuweisen. Gehen Sie dann wie unter dem Punkt **a)** beschrieben vor.

   Das erneute Zuweisen der Active Directory-basierte Richtlinien kann dabei auf eine für Sie bequeme Weise erfolgen.

2.4. NAP Validator installieren

Mit der Komponente **Dr.Web NAP Validator** können Sie die Funktionsfähigkeit der Antivirensoftware auf den zu schützenden Workstations überprüfen.

Diese Komponente wird auf einem Rechner mit dem konfigurierten NAP-Server installiert.

So installieren Sie die Komponente NAP Validator

1. Starten Sie die Distributionsdatei. Es öffnet sich das Fenster zur Auswahl der Sprache für den Installationsprozess. Wählen Sie **Deutsch** und klicken Sie auf **Weiter**.
2. Es öffnet sich das Fenster **InstallShield Wizard** mit Informationen zum zu installierenden Produkt. Klicken Sie die Schaltfläche **Weiter** an.
3. Als nächstes Fenster erscheint die Lizenzvereinbarung. Nachdem Sie sich mit den Bedingungen der Lizenzvereinbarung vertraut gemacht haben, wählen Sie **Ich akzeptiere die Bedingungen der Lizenzvereinbarung** aus und klicken Sie auf **Weiter**.
4. Geben Sie im geöffneten Fenster in die Felder **Adresse** und **Port** die IP-Adresse und den Port des **Dr.Web Servers** ein. Klicken Sie auf **Weiter**.
5. Klicken Sie auf **Installieren**. Weitere Aktionen des Installationsprogramms benötigen keine weiteren Eingriffe durch Benutzer.
6. Nachdem die Installation abgeschlossen ist, klicken Sie auf **Fertig**.

Nachdem die Komponente **Dr.Web NAP Validator** installiert ist, muss der **Dr.Web Server** in die Gruppe vertrauenswürdiger NAP-Server aufgenommen werden. Gehen Sie dafür so vor:

1. Öffnen Sie die Konfigurationskomponente des NAP-Servers (führen Sie den Befehl `nps.msc` aus).
2. Klicken Sie im Bereich **Wartungsservergruppen** auf **Hinzufügen**.
3. Geben Sie im geöffneten Dialogfeld den Namen für den Wartungsserver sowie die IP-Adresse des **Dr.Web Servers** an.
4. Um die vorgenommenen Änderungen zu übernehmen, klicken Sie auf **OK**.

2.5. Proxy-Server installieren

Ein Antivirus-Netzwerk kann ein bzw. mehrere **Proxy-Server** umfassen.

Das entscheidendste Kriterium für die Auswahl des Rechners, auf dem der **Proxy-Server** installiert werden soll, ist die Voraussetzung, dass der **Proxy-Server** für alle Netzwerke/Segmente der Netzwerke, zwischen denen er Informationen weiterreichen wird, verfügbar sein muss.

Die Installation des **Proxy-Servers** muss von einem Benutzer dieses Rechners durchgeführt werden, der administrative Rechte besitzt.

Um eine sichere Kommunikation zwischen dem **Server** und Clients über den **Proxy-Server** zu ermöglichen, empfehlen wir Ihnen, die Verschlüsselung des Datenverkehrs zu deaktivieren. Wählen Sie dafür den Wert **Nein** für den Parameter **Verschlüsselung** im Bereich **Dr.Web Server-Konfiguration** aus (mehr dazu finden Sie im **Administratorhandbuch** unter Dr.Web Server konfigurieren > Allgemein).

Im Nachfolgenden wird die Installation des **Proxy-Servers** beschrieben. Die Zahl sowie die Reihenfolge der Schritte können je nach Distributionsversion variieren.

So installieren Sie den Proxy-Server auf einem Rechner unter Windows

1. Starten Sie die Distribution. Es öffnet sich das Fenster **InstallShield Wizard** mit Informationen zum zu installierenden Produkt. Klicken Sie die Schaltfläche **Weiter** an.

2. Als nächstes Fenster erscheint die Lizenzvereinbarung. Nachdem Sie sich mit den Bedingungen der Lizenzvereinbarung vertraut gemacht haben, wählen Sie **Ich akzeptiere die Bedingungen der Lizenzvereinbarung** aus und klicken Sie auf **Weiter**.
3. Es öffnet sich ein Fenster, in dem die wichtigsten Einstellungen des **Proxy-Servers** konfiguriert werden:
   - Legen Sie im Feld **Listen to** eine IP-Adresse fest, an der der **Proxy-Server** lauschen soll. Standardmäßig – `any (0.0.0.0)` – alle Schnittstellen werden abgehört.

Die Adressen müssen im Format von Netzwerkadressen angegeben werden. Die erlaubten Schreibweisen finden Sie im Dokument **Anhänge** unter Anhang E. Spezifikation zur Schreibweise von Netzwerkadressen.

   - Legen Sie im Feld **Port** die Nummer des Ports, an dem der**Proxy-Server** lauschen wird. Standardmäßig – **2193**.
   - Aktivieren Sie das Kontrollkästchen **Enable discovery**, um den **Server** im Simulationsmodus zu starten. In diesem Modus lässt sich der **Proxy-Server** als **Dr.Web Server** erkennen. Für den Simulationsmodus des **Servers** sind die folgenden Einstellungen verfügbar:
     - Aktivieren Sie das Kontrollkästchen **Enable multicasting**, damit der **Proxy-Server** auf Broadcastanforderungen für den **Server** antworten kann.
     - Im Feld **Multicast group** legen Sie die IP-Adresse der Multicastgruppe fest, zu welcher der **Proxy-Server** gehören wird. Die angegebene Schnittstelle wird vom **Proxy-Server** für die Kommunikation mit den **Netzwerk-Installern** bei der Suche nach aktiven **Dr.Web Servern** abgehört. Wenn Sie das Feld leer lassen, wird der **Proxy-Server** in keine Multicastgruppe aufgenommen. Standardmäßig gehört der **Server** der Multicastgruppe `231.0.0.1`.
   - Wählen Sie in der Dropdown-Liste **Compression mode** einen Komprimierungsmodus für den Datenverkehr zwischen dem **Proxy-Server** und Clients: **Agents** und Installationsprogrammen der **Agents**. Legen Sie im Feld **Level** den gewünschten Komprimierungsgrad fest. Dabei dürfen nur ganze Zahlen zwischen 1 bis 8 eingegeben werden.

   Nachdem die wichtigsten Einstellungen festgelegt sind, klicken Sie auf **Next**.

4. Es öffnet sich das Fenster mit Einstellungen für die Zwischenspeicherung durch den **Proxy-Server**:

   Aktivieren Sie das Kontrollkästchen **Enable caching**, um die Daten zwischenzuspeichern, die vom **Proxy-Server** übertragen werden, und legen Sie anschließend die folgenden Einstellungen fest:

   - Um das Standard-Verzeichnis zum Speichern der Daten, die zwischengespeichert werden sollen, zu ändern, klicken Sie auf **Browse** und wählen Sie im Dateisystem-Browser ein anderes Verzeichnis aus.
   - Legen Sie im Feld **Maximum revisions number** die maximal zulässige Anzahl der gespeicherten Revisionen fest. Standardmäßig werden 3 letzte Revisionen gespeichert, alle älteren Revisionen werden gelöscht.
   - Legen Sie im Feld **Cleanup interval** das Intervall (in Minuten) zwischen dem Löschen von älteren Revisionen fest (standardmäßig 60 Minuten).
   - Legen Sie im Feld **Unload interval** das Intervall (in Minuten) fest, in dem nicht verwendete Dateien aus dem Arbeitsspeicher entladen werden sollen (standardmäßig 10 Minuten).
   - Wählen Sie in der Dropdown-Liste **Integrity check mode** einen Modus für die Überprüfung der Integrität des Cache:
     - **At startup** – beim Starten des **Proxy-Servers** (dieser Vorgang dauert möglicherweise einige Minuten).
     - **Idle** – im Hintergrund, solange der **Proxy-Server** läuft.

   Nachdem die Cacheeinstellungen festgelegt sind, klicken Sie auf **Next**.

5. Es öffnet sich das Fenster mit Einstellungen für die Umleitung von Verbindungen:

   Legen Sie im Abschnitt **Redirection settings** die Adresse oder Liste der Adressen des **Dr.Web Servers** fest, auf welche die vom **Proxy-Server** hergestellten Verbindungen umgeleitet werden sollen.

   Die Adressen müssen im Format von Netzwerkadressen angegeben werden. Die erlaubten Schreibweisen finden Sie im Dokument **Anhänge** unter Anhang E. Spezifikation zur Schreibweise von Netzwerkadressen.

   Wählen Sie in den Dropdown-Listen **Compression mode** Komprimierungsmodi für die Kommunikation zwischen dem **Proxy-Server** und jedem der angegebenen **Dr.Web Server** aus.

   Nachdem die Umleitungseinstellungen festgelegt sind, klicken Sie auf **Next**.

6. Es öffnet sich das Fenster zur Auswahl des Installationsverzeichnisses. Wenn Sie das Standard-Installationsverzeichnis ändern möchten, klicken Sie auf **Change** und wählen Sie das gewünschte Installationsverzeichnis aus.

   Klicken Sie auf **Next**.

7. Sobald der **Proxy-Server** zur Installation bereit ist, erscheint ein entsprechendes Fenster. Um mit der Installation des **Proxy-Servers** zu beginnen, klicken Sie auf **Install**.
8. Nachdem die Installation abgeschlossen ist, klicken Sie auf **Finish**.

Nachdem die Installation abgeschlossen ist, können Sie die Einstellungen des **Proxy-Servers** jederzeit ändern. Verwenden Sie dazu die Konfigurationsdatei `drwcsd-proxy.xml`, die sich im Installationsverzeichnis des **Proxy-Server** befindet. Die Beschreibung der in der Konfigurationsdatei enthaltenen Einstellungen finden Sie im Dokument **Anhänge** unter Anhang G4.

So installieren Sie den Proxy-Server auf einem Rechner unter einem UNIX-artigen Betriebssystem

Führen Sie den folgenden Befehl aus:

```
sh ./<Distributionsdatei>.run
```

Bei der Installation der Software unter **FreeBSD** wird das `rc`-Skript `/usr/local/etc/rc.d/0.dwcp-proxy.sh` erstellt.

Verwenden Sie die folgenden Befehle:

- `/usr/local/etc/rc.d/0.dwcp-proxy.sh stop` – um den **Proxy-Server** manuell zu stoppen.
- `/usr/local/etc/rc.d/0.dwcp-proxy.sh start` – um den **Proxy-Server** manuell zu starten.

Bei der Installation der Software unter **Linux** und **Solaris** wird das `init`-Skript zum Starten und Stoppen des **Proxy-Servers** `/etc/init.d/dwcp-proxy` erstellt.

Kapitel 3: Komponenten von Dr.Web Enterprise Security Suite deinstallieren

3.1. Deinstallieren von Dr.Web Server

3.1.1. Dr.Web Server unter Windows® deinstallieren

Um die Software des **Dr.Web Servers** (der Basisdistribution und zusätzlichen Distribution) oder der Browser-Erweiterung für das **Dr.Web Sicherheitscenter** zu deinstallieren, starten Sie das Installationspaket derjenigen Produktversion, die auf Ihrem Rechner installiert wurde. Das Installationsprogramm wird automatisch das Produkt bestimmen und Sie auffordern, es zu deinstallieren. Um die Software zu deinstallieren, klicken Sie auf **Entfernen**.

Die Software des **Dr.Web Servers** (der Basisdistribution und zusätzlichen Distribution) oder der Browser-Erweiterung für das **Dr.Web Sicherheitscenter** lassen sich auch mit Windows-Bordmitteln deinstallieren. Wechseln Sie dafür zu **Systemsteuerung** → **Software**.

3.1.2. Dr.Web Server unter Betriebssystemen der UNIX®-Familie deinstallieren

Die Deinstallation kann nur vom Super-User (**root**) ausgeführt werden.

Basisdistribution vom Dr.Web Server deinstallieren

1. Die Vorgehensweise für die Deinstallation des **Servers** hängt jeweils vom Betriebssystem und von der installierten Version des **Servers** ab.

   a) Um einen **Server** der Version **6.XX** oder niedriger zu deinstallieren, gehen Sie so vor:

Betriebssystem des Servers		Aktion
FreeBSD		Führen Sie den folgenden Befehl aus: `pkg_delete drweb-esuite`
Solaris		1. Stoppen Sie den **Server**: `/etc/init.d/drwcsd stop` 2. Führen Sie den folgenden Befehl aus: `pkgrm DWEBesuit`
Linux	Debian Ubuntu	Führen Sie den folgenden Befehl aus: `dpkg -r drweb-esuite`
	rpm-Paket	Führen Sie den folgenden Befehl aus: `rpm -e drweb-esuite`
	generic-Paket	Führen Sie dieses Skript aus `/opt/drwcs/bin/drweb-esuite-uninstall.sh`

   b) Um einen **Server** der Version **10.0** zu deinstallieren, gehen Sie so vor:

Betriebssystem des Servers	Aktion
FreeBSD	Führen Sie dieses Skript aus `/usr/local/etc/opt/software/drweb-esuite.remove`

Betriebssystem des Servers		Aktion
Solaris		1. Stoppen Sie den **Server**: `/etc/init.d/drwcsd stop` 2. Führen Sie den folgenden Befehl aus: `pkgrm drweb-esuite`
Linux	Debian Ubuntu	Führen Sie den folgenden Befehl aus: `dpkg -P drweb-esuite`
	rpm-Paket	Führen Sie den folgenden Befehl aus: `rpm -e drweb-esuite`
	generic-Paket	Führen Sie dieses Skript aus `/etc/opt/drweb.com/software/drweb-esuite.remove`

2. Bei der Deinstallation unter **Solaris** werden Sie aufgefordert, die Deinstallation der Software zu bestätigen sowie der Ausführung der Deinstallationsskripts mit root-Rechten (**root**) zuzustimmen.

Bei der Deinstallation des **Servers** unter **FreeBSD** und **Linux** werden sämtliche Servervorgänge automatisch beendet. Die Datenbank, Schlüssel- und Konfigurationsdateien werden ins Standardverzeichnis `/var/tmp/drwcs` kopiert.

Zusätzliche Distribution des Dr.Web Servers deinstallieren

1. Um die zusätzliche Distribution des **Servers** der Version **10.0** zu deinstallieren, gehen Sie so vor:

Betriebssystem des Servers		Aktion
FreeBSD		Führen Sie dieses Skript aus `/usr/local/etc/opt/software/drweb-esuite-extra.remove`
Solaris		1. Stoppen Sie den **Server**: `/etc/init.d/drwcsd stop` 2. Führen Sie den folgenden Befehl aus: `pkgrm drweb-esuite-extra`
Linux	Debian Ubuntu	Führen Sie den folgenden Befehl aus: `dpkg -P drweb-esuite-extra`
	rpm-Paket	Führen Sie den folgenden Befehl aus: `rpm -e drweb-esuite-extra`
	generic-Paket	Führen Sie dieses Skript aus `/etc/opt/drweb.com/software/drweb-esuite-extra.remove`

2. Bei der Deinstallation unter **Solaris** werden Sie aufgefordert, die Deinstallation der Software zu bestätigen sowie der Ausführung der Deinstallationsskripts mit root-Rechten (**root**) zuzustimmen.

Browser-Erweiterung für das Dr.Web Sicherheitscenter deinstallieren

Um die Browser-Erweiterung für das **Dr.Web Sicherheitscenter** zu deinstallieren, führen Sie den folgenden Befehl:

Pakettyp	Befehl
deb-Paket	`dpkg -P drweb-esuite-plugins`
rpm-Paket	`rpm -e drweb-esuite-plugins`

Sonstige Pakete (**tar.bz2** und **tar.gz**)	`rm -f <`*Verzeichnis_für_Plugins*`>/libnp*.so`
	Beispiel für Mozilla Firefox Webbrowser:
	`rm -f /usr/lib/mozilla/plugins/libnp*.so`

3.2. Dr.Web Agent deinstallieren

Die Deinstallation der auf den Workstations installierten **Dr.Web Agents** kann über die folgenden Wege erfolgen:

- Für Workstations unter Windows:
  - Remote-Deinstallation über das Verwaltungscenter.
  - Lokale Deinstallation an der Workstation.
  - Über Active Directory, sofern der **Agent** über diesen Windows-Dienst installiert wurde.
- Für Workstations unter Android, Linux, Mac OS X erfolgt die Deinstallation lokal.

Die Deinstallation des **Dr.Web Agents** auf Workstations unter Android, Linux, Mac OS X wird im **Benutzerhandbuch** für das jeweilige Betriebssystem beschrieben.

3.2.1. Dr.Web Agent unter Windows® deinstallieren

Dr.Web Agent und Antivirenpaket remote deinstallieren

Die Remote-Deinstallation der Software des **Agents** ist nur innerhalb von einem lokalen Netzwerk möglich und benötigt Administratorrechte.

Wenn die Deinstallation des **Agents** und Antivirenpakets über das **Verwaltungscenter** erfolgt, wird die **Quarantäne** der Workstation nicht entfernt.

So deinstallieren Sie die Antivirensoftware auf der Workstation remote (nur unter Windows)

1. Wählen Sie im Hauptmenü vom **Verwaltungscenter** den Punkt **Antivirus-Netzwerk**.
2. Wählen Sie im geöffneten Fenster die gewünschte Gruppe von Workstations bzw. einzelne Workstations aus.
3. Klicken Sie in der Symbolleiste des Antivirus-Netzwerks auf **Allgemein** → **Dr.Web Agent deinstallieren**.
4. Die Software des **Agents** und das Antivirenpaket werden von den ausgewählten Workstations entfernt.

Wenn beim Start der Deinstallation keine Verbindung zwischen dem **Dr.Web Server** und der Workstation besteht, wird die Software des **Agents** auf der gewählten Workstation erst dann deinstalliert, sobald eine Verbindung wieder hergestellt wird.

Dr.Web Agent und Antivirenpaket lokal deinstallieren

Um den **Agent** und das Antivirenpaket lokal deinstallieren zu können, müssen Sie vorab die entsprechende Option auf dem **Server** im Bereich **Rechte** aktivieren (mehr dazu finden Sie im **Administratorhandbuch** unter Benutzerrechte konfigurieren).

Die Deinstallation der Workstation-Antivirensoftware (des **Agents** und Antivirenpakets) kann auf zwei Weisen erfolgen:

1. Mit Windows-Bordmitteln.
2. Mithilfe des Installationsprogramms vom Agent.

> Wenn der **Agent** und das Antivirenpaket mit Windows-Bordmitteln bzw. mithilfe des Installationsprogramms vom **Agent** deinstalliert werden, wird der Benutzer aufgefordert, die **Quarantäne** zu entfernen.

Deinstallation mit Windows-Bordmitteln

> Diese Methode ist nur dann anwendbar, wenn das Kontrollkästchen **Dr.Web Agent in der Liste der installierten Programme registrieren** bei der Installation des **Agents** im Grafikmodus aktiviert wurde.
>
> Wenn der **Agent** im Hintergrundmodus installiert wurde, ist die Deinstallation der Antivirensoftware mit Windows-Bordmitteln nur dann möglich, falls bei der Installation der Schalter `/regagent yes` verwendet wurde.

Um den **Agent** und das Antivirenpaket mit Windows-Bordmitteln zu deinstallieren, wechseln Sie zu **Systemsteuerung** → **Software** (die detaillierte Beschreibung finden Sie im **Benutzerhandbuch** für **Dr.Web Agent für Windows**).

Deinstallation mithilfe des Installationsprogramms

- **Client-Modul win-es-agent-setup.exe**

  Um die Software des **Agents** und das Antivirenpaket mithilfe des Client-Moduls, das bei der Installation des **Agents** generiert wird, zu deinstallieren, führen Sie die Installationsdatei `win-es-agent-setup.exe` mit dem Parameter `/instMode remove` aus. Wenn Sie den Vorgang steuern wollen, verwenden Sie den zusätzlichen Parameter `/silent no`.

  Die Installationsdatei `win-es-agent-setup.exe` befinden sich standardmäßig im folgenden Verzeichnis:

  - Für Windows XP und Windows Server 2003:
    `%ALLUSERSPROFILE%\Application Data\Doctor Web\Setup\`
  - Für Windows Vista und höher, Windows Server 2008 und höher:
    `%ALLUSERSPROFILE%\Doctor Web\Setup\`

  Für Windows 7, `%ALLUSERPROFILE%` entspricht `C:\ProgramData`:

  ```
  C:\ProgramData\Doctor Web\Setup\win-es-agent-setup.exe /instMode remove /silent no
  ```

- **Installationspaket drweb-esuite-install.exe**

  Um die Software des **Agents** und das Antivirenpaket mithilfe des Installationsprogramms zu deinstallieren, führen Sie die Installationsdatei `drweb-esuite-install.exe` der installierten Produktversion aus.

- **Vollversion des Installationsprogramms drweb-esuite-agent-full-10.00.0-<*Buildversion*>-windows.exe**

  Um die Software des **Agents** und das Antivirenpaket mithilfe der Vollversion des Installationsprogramms zu deinstallieren, führen Sie die Installationsdatei `drweb-esuite-agent-full-10.00.0-<Buildversion>-windows.exe` der installierten Produktversion aus.

- **Netzwerk-Installer drwinst.exe**

  Um die Software des **Agents** und das Antivirenpaket mithilfe des Netzwerk-Installers auf der Workstation lokal zu deinstallieren, starten Sie im Installationsverzeichnis des **Dr.Web Agents** (standardmäßig `C:\Program Files\DrWeb`) das Installationsprogramm `drwinst.exe` mit dem Parameter `/instMode remove`. Wenn Sie den Vorgang steuern wollen, verwenden Sie den zusätzlichen Parameter `/silent no`.

  Beispiel:

```
drwinst /instMode remove /silent no
```

Beim Start des Installationspakets `drweb-esuite-install.exe`, der Vollversion des Installationsprogramms `drweb-esuite-agent-full-10.00.0-<Buildversion>-windows.exe` und des Netzwerk-Installers `drwinst.exe` wird die Deinstallation durch das Client-Modul `win-es-agent-setup.exe` durchgeführt.

Wenn das Client-Modul `win-es-agent-setup.exe` ohne Parameter gestartet wird, erkennt es das installierte Produkt und wird im Ändern/Entfernen-Modus gestartet. Um das Installationsprogramm direkt im Entfernen-Modus zu starten, verwenden Sie den Schalter `/instMode remove`.

3.2.2. Dr.Web Agent über Active Directory deinstallieren

1. Öffnen Sie in der Windows-Systemsteuerung das Menü **Verwaltung** und wählen Sie dort **Active Directory-Benutzer und -Computer**.
2. Wählen Sie in der Domäne die von Ihnen erstellte Organisationseinheit **ESS** aus. Wählen Sie im Kontextmenü **Eigenschaften**. Es öffnet sich das Fenster **Eigenschaften von ESS**.
3. Wechseln Sie zur Registerkarte **Gruppenrichtlinie**. Wählen Sie den Eintrag mit dem Namen **Richtlinien von ESS**. Doppelklicken Sie darauf. Es öffnet sich das Fenster **Gruppenrichtlinienobjekt-Editor**.
4. Wählen Sie in der hierarchischen Struktur **Computerkonfiguration** → **Softwareeinstellungen** → **Softwareinstallation** → **Paket**. Wählen Sie dann im Kontextmenü vom Distributionspaket des **Agents** den Menüpunkt **Alle Aufgaben** → **Entfernen** → **OK**.
5. Klicken Sie auf der Registerkarte **Gruppenrichtlinie** auf **OK**.
6. **Dr.Web Agent** wird von den Rechnern bei der nächsten Registrierung in der Domäne deinstalliert.

3.3. Proxy-Server entfernen

Proxy-Server unter Windows entfernen

Bei der Deinstallation des **Proxy-Servers** wird auch die Konfigurationsdatei `drwcsd-proxy.xml` gelöscht. Speichern Sie bei Bedarf die Konfigurationsdatei manuell ab, bevor Sie mit der Deinstallation des **Proxy-Servers** beginnen.

Die Software des **Proxy-Servers** lässt sich auch mit Windows-Bordmitteln entfernen. Dafür wechseln Sie zu **Systemsteuerung** → **Software** (**Programme und Funktionen** für Windows 2008).

Proxy-Server unter UNIX-artigen Betriebssystemen entfernen

Betriebssystem des Proxy-Servers		Aktion
FreeBSD		Führen Sie dieses Skript aus `/usr/local/etc/opt/software/drweb-proxy.remove`
Solaris		Führen Sie den folgenden Befehl aus: `pkgrm drweb-esuite-proxy`
Linux	deb-Paket	Führen Sie den folgenden Befehl aus: `dpkg -P drweb-esuite-proxy`
	rpm-Paket	Führen Sie den folgenden Befehl aus: `rpm -e drweb-esuite-proxy`
	generic-Paket	Führen Sie dieses Skript aus `/etc/opt/drweb.com/software/drweb-proxy.remove`

Kapitel 4: Komponenten von Dr.Web Enterprise Security Suite aktualisieren

Bevor Sie mit der Aktualisierung der **Dr.Web Enterprise Security Suite** und ihrer einzelnen Komponenten anfangen, nehmen Sie die folgenden Informationen zur Kenntnis:

- Bevor Sie mit der Aktualisierung beginnen, sollten Sie sicherstellen, dass Sie über eine aktive Internetverbindung verfügen und das TCP/IP-Protokoll richtig konfiguriert haben. Überprüfen Sie vor allem, dass der DNS-Dienst aktiviert und richtig konfiguriert ist.
- Wenn das Antivirus-Netzwerk aus mehreren **Servern** besteht, müssen Sie berücksichtigen, dass zwischen den **Servern** der Version **10.0** und **Servern** der Version **6.XX** keine Updates übertragen werden können. Diese Server-zu-Server-Kommunikation wird nur für den Austausch statistischer Informationen verwendet. Damit Updates zwischen allen **Servern** übertragen werden können, müssen sie aktualisiert werden. Wenn Sie einige **Server** im Antivirus-Netzwerk nicht auf eine neuere Version aktualisiert wollen, z. B. damit **Agents** unter einem der in der Version **10.0** nicht mehr unterstützten Betriebssysteme verbunden werden können (s. Dr.Web Agents aktualisieren), müssen die **Server** der Version **6.XX** und **Server** der Version **10.0** ihre Updates unabhängig voneinander beziehen.
- Bei der Aktualisierung des **Servers** von der Version **6.XX** auf die Version **10.0** gehen die Proxy-Einstellungen des **Servers** verloren. Sobald die Version **10.0** erfolgreich installiert ist, müssen diese Proxy-Einstellungen manuell festgelegt werden (mehr dazu finden Sie im **Administratorhandbuch** unter Proxy).
- Während der automatischen Aktualisierung der **Agents** wird die alte Version des jeweiligen **Agents** durch eine neuere ersetzt. Die Installation einer neueren Version des **Agents** erfolgt entsprechend der Aufgabe im Zeitplan des **Servers**, die nach dem Neustart der Workstation ausgeführt wird. Die Workstation muss manuell neu gestartet werden, sobald die alte Version des **Agents** deinstalliert ist.

Da Benutzer auf der Workstation nach der Deinstallation des **Agents** nicht zum Neustart aufgefordert werden, muss der Administrator den Neustart selbst initiieren.

Im Zeitraum von der Deinstallation der alten Version des **Agents** bis zur Installation einer neueren Version sind die Workstations vor Schadsoftware nicht geschützt.

4.1. Dr.Web Server unter Windows® aktualisieren

Das Update des **Servers** von der Version **6** auf die Version **10** und innerhalb der Versionsnummer **10** erfolgt automatisch mithilfe des Installationsprogramms.

Bevor Sie mit der Deinstallation des **Servers** der vorherigen Version beginnen, lesen Sie den Abschnitt Dr.Web Agent aktualisieren aufmerksam durch.

Das Update des **Servers** innerhalb der Versionsnummer **10** kann auch über das **Verwaltungscenter** durchgeführt werden. Die Vorgehensweise beim Update ist im **Administratorhandbuch** unter Dr.Web Server aktualisieren und aus einer Sicherungskopie wiederherstellen zu finden.

Einige Updates des **Servers** innerhalb der Versionsnummer **10** enthalten keine Distributionsdatei. Aus diesem Grund können einige von ihnen nur über das **Verwaltungscenter** installiert werden.

Konfigurationsdateien speichern

Bei der Deinstallation des **Servers** der Version **6.X** werden die folgenden Dateien automatisch gespeichert:

Datei	Erläuterung	Verzeichnis
`agent.key` (der Name kann abweichen)	Lizenzschlüssel des **Agents**	`etc`
`certificate.pem`	SSL-Zertifikat	
`drwcsd.conf` (der Name kann abweichen)	Konfigurationsdatei des **Servers**	
`drwcsd.pri`	Privater Schlüssel	
`enterprise.key` (der Name kann abweichen)	Lizenzschlüssel des **Servers**	
`private-key.pem`	Privater RSA-Schlüssel	
`auth-ads.xml`	Konfigurationsdatei für die externe Active Directory-Autorisierung der Administratoren	
`auth-ldap.xml`	Konfigurationsdatei für die externe LDAP-Autorisierung der Administratoren	
`auth-radius.xml`	Konfigurationsdatei für die externe RADIUS-Autorisierung der Administratoren	
`dbinternal.dbs`	Eingebettete Datenbank	`var`
`drwcsd.pub`	Öffentlicher Schlüssel	• `Installer` • `webmin\install`

Bei der Deinstallation des **Servers** der Version **10.0** werden folgende Konfigurationsdateien gespeichert:

Datei	Erläuterung	Verzeichnis
`agent.key` (der Name kann abweichen)	Lizenzschlüssel des **Agents**	`etc`
`enterprise.key` (der Name kann abweichen)	Lizenzschlüssel des **Servers**. Die Datei wird gespeichert, falls sie nach der Aktualisierung von älteren Versionen geblieben ist. Die Datei fehlt im neuen **Server 10.0**	
`frontdoor.conf`	Konfigurationsdatei für das Dienstprogramm zur Ferndiagnose des **Servers**	
`proxy.conf`	Konfigurationsdatei des Proxy-Servers	
`auth-ads.xml`	Konfigurationsdatei für die externe Active Directory-Autorisierung der Administratoren	
`auth-ldap.xml`	Konfigurationsdatei für die externe LDAP-Autorisierung der Administratoren	
`auth-radius.xml`	Konfigurationsdatei für die externe RADIUS-Autorisierung der Administratoren	
`download.conf`	Netzwerkeinstellungen für die Generierung der Installationspakete des **Agents**	
`drwcsd.conf` (der Name kann abweichen)	Konfigurationsdatei des **Servers**	

Datei	Erläuterung	Verzeichnis
drwcsd.conf.distr	Muster der Konfigurationsdatei des **Servers** mit Standardparametern	
drwcsd.pri	Privater Schlüssel	
openssl.cnf	Zertifikat des **Servers** für HTTPS	
webmin.conf	Konfigurationsdatei des **Verwaltungscenters**	
dbexport.gz	Datenbank exportieren	Verzeichnis *<backup>*
drwcsd.pub	Öffentlicher Schlüssel	• Installer • webmin\install

Wenn Sie die Konfigurationsdateien des **Servers** der vorherigen Version verwenden wollen, beachten Sie das Folgende:

1. Lizenzschlüssel des **Servers** werden nicht mehr verwendet (mehr dazu finden Sie unter Lizenzierung).
2. Die eingebettete Datenbank wird aktualisiert, und die Konfigurationsdatei des **Servers** wird mithilfe des Installationsprogramms konvertiert. Diese Dateien müssen beim Update des **Servers** auf die Version **10.0** nicht ersetzt werden.

Sichern Sie bei Bedarf andere wichtige Dateien an einem beliebigen Ort (aber nicht im Installationsverzeichnis des **Servers**): z. B. Berichtsvorlagen, die sich im Verzeichnis `\var\templates` befinden.

Datenbank speichern

Microsoft SQL Server-Datenbanken werden auf dem **Dr.Web Server 10.0** nicht mehr unterstützt. Beim automatischen Update des **Servers** wird die Microsoft SQL Server-Datenbank mithilfe des Installationsprogramms in die IntDB-Datenbank konvertiert.

Wir empfehlen Ihnen, vor der Aktualisierung der Software von **Dr.Web Enterprise Security Suite** eine Sicherungskopie der Datenbank zu erstellen.

So speichern Sie Ihre Datenbank

1. Beenden Sie den **Server**.
2. Exportieren Sie die Datenbank in die Datei:

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -verbosity=all exportdb <Verzeichnis_der_Sicherungskopie>\esbase.es
```

Es empfiehlt sich, für die **Server**, die eine externe Datenbank verwenden, die mit der Datenbank mitgelieferten Tools zu verwenden.

Stellen Sie sicher, dass die Datenbank von **Dr.Web Enterprise Security Suite** erfolgreich exportiert wurde. Wenn keine Sicherungskopie der Datenbank erstellt wurde, können Sie den **Server** nicht mehr wiederherstellen.

Dr.Web Server aktualisieren

So aktualisieren Sie den Dr.Web Server

1. Starten Sie die Distributionsdatei. Das Fenster zur Auswahl der Sprache für den Installationsprozess wird angezeigt. Wählen Sie **Deutsch** und klicken Sie auf **Weiter**.
2. Wenn auf dem Rechner, auf dem Sie den **Dr.Web Server** installieren, ein **Dr.Web Agent** mit der aktivierten Selbstschutzfunktion bereits installiert ist, wird eine Meldung über die aktivierte **Dr.Web** Selbstschutzfunktion ausgegeben. Deaktivieren Sie diese Komponente über die Einstellungen des **Agents** und klicken Sie auf **OK**, um den Vorgang fortzusetzen, bzw. auf **Abbrechen**, um das Update des **Servers** abzubrechen.
3. Das Fenster **InstallShield Wizard** mit Informationen zum zu installierenden Produkt wird geöffnet. Klicken Sie die Schaltfläche **Weiter** an.
4. Das Fenster **Dr.Web Server Anmerkungen zum Upgrade**, das Sie von der installierten Software des **Servers** einer älteren Version informiert, wird angezeigt.

   Das Installationsprogramm findet automatisch das Installationsverzeichnis des **Servers**, die Konfigurationsdateien und eingebettete Datenbank der vorherigen Installation.

   Klicken Sie auf **Weiter**.
5. Als nächstes Fenster erscheint die Lizenzvereinbarung. Nachdem Sie sich mit den Bedingungen der Lizenzvereinbarung vertraut gemacht haben, wählen Sie **Ich akzeptiere die Bedingungen der Lizenzvereinbarung**, um das Update fortzusetzen, und klicken Sie anschließend auf **Weiter**.
6. In den nächsten Schritten müssen Sie die Einstellungen für den zu aktualisierenden **Server**, wie im Dr.Web Server installieren beschrieben, anhand der Konfigurationsdateien der vorherigen Version (s. oben) festlegen. Sie können bei Bedarf die Pfade der vom Installationsprogramm gefundenen Dateien manuell ändern.

Wenn Sie eine externe Datenbank für den **Server** verwenden, wählen Sie die Option **Vorhandene Datenbank benutzen**.

Wenn Sie als externe Datenbank eine Oracle- oder PostgreSQL-Datenbank, auf die über eine ODBC-Verbindung zugegriffen werden soll, verwenden wollen, muss bei der Aktualisierung des **Servers** in den Einstellungen des Installationsprogramms der Punkt **Benutzerdefiniert** ausgewählt werden und dann im nächsten Fenster die Installation des entsprechenden integrierten DBMS-Clients (im Bereich **Database support**) deaktiviert werden.

Anderenfalls kann auf die Oracle-Datenbank über die ODBC-Verbindung aufgrund eventueller Probleme durch inkompatible Bibliotheken nicht zugegriffen werden.

7. Um mit der Deinstallation des **Servers** der vorherigen Version und mit der anschließenden Installation des **Servers** der Version**10.0** zu beginnen, klicken Sie auf **Installieren**.

Nachdem die **Server** des Antivirus-Netzwerks aktualisiert wurden, müssen die Verschlüsselungs- und Komprimierungseinstellungen auf den verbundenen **Servern** (mehr dazu finden Sie im **Administratorhandbuch** unter Verbindungen zwischen Servern konfigurieren) neu konfiguriert werden.

Damit das Verwaltungscenter seine Aufgaben wieder funktionsgerecht bewältigen kann, müssen Sie nach der Aktualisierung der Software des Dr.Web Servers die folgenden Aktionen durchführen:

1. Löschen Sie den Cache aus dem Speicher des Webbrowsers, den Sie für die Verbindung mit dem **Verwaltungscenter** verwendet haben.
2. Aktualisieren Sie die Browser-Erweiterung für das **Dr.Web Sicherheitscenter**.

4.2. Dr.Web Server unter Betriebssystemen der UNIX®-Familie aktualisieren

Die Aktualisierung kann nur vom Super-User (**root**) ausgeführt werden.

Das automatische Update vorheriger Versionen des **Servers** auf die Version **10** ohne vorherige Deinstallation der vorhandenen Version ist leider nicht für alle UNIX-artigen Betriebssysteme möglich. Um die Server-Software unter diesen Betriebssystemen auf den aktuellen Stand zu bringen, müssen Sie zuerst eine Sicherungskopie der Software des **Servers** der alten Version speichern, die vorhandene Software deinstallieren und abschließend die Software der Version **10.0** auf Basis der gespeicherten Sicherungskopie installieren.

Das Update des **Servers** innerhalb der Version **10** erfolgt für die gleichen Pakettypen unter allen UNIX-basierten Betriebssystemen automatisch.

Bevor Sie mit der Deinstallation des **Servers** der vorherigen Version beginnen, lesen Sie den Abschnitt Dr.Web Agent aktualisieren aufmerksam durch.

Das Update des **Servers** innerhalb der Versionsnummer **10** kann auch über das **Verwaltungscenter** durchgeführt werden. Die Vorgehensweise beim Update ist im **Administratorhandbuch** unter Dr.Web Server aktualisieren und aus einer Sicherungskopie wiederherstellen zu finden.

Einige Updates des **Servers** innerhalb der Versionsnummer **10** enthalten keine Distributionsdatei. Aus diesem Grund können einige von ihnen nur über das **Verwaltungscenter** installiert werden.

Konfigurationsdateien speichern

Bei der Deinstallation des **Servers** der Version **6.X** werden die folgenden Dateien automatisch gespeichert:

Datei	Erläuterung	Standardverzeichnis
`agent.key` (der Name kann abweichen)	Lizenzschlüssel des **Agents**	• Für Linux und Solaris: /var/opt/drwcs/etc • Für FreeBSD: /var/drwcs/etc
`certificate.pem`	SSL-Zertifikat	
`download.conf`	Netzwerkeinstellungen für die Generierung der Installationspakete des **Agents**	
`drwcsd.conf` (der Name kann abweichen)	Konfigurationsdatei des **Servers**	
`drwcsd.pri`	Privater Schlüssel	
`enterprise.key` (der Name kann abweichen)	Lizenzschlüssel des **Servers**	
`private-key.pem`	Privater RSA-Schlüssel	
`webmin.conf`	Konfigurationsdatei des **Verwaltungscenters**	
`common.conf`	Konfigurationsdatei (für einige UNIX-ähnliche Betriebssysteme)	

Datei	Erläuterung	Standardverzeichnis
local.conf	Einstellungen vom Protokoll des **Servers**	
dbinternal.dbs	Eingebettete Datenbank	• Für Linux und Solaris: /var/opt/drwcs/ • Für FreeBSD: /var/drwcs/
drwcsd.pub	Öffentlicher Schlüssel	• Für Linux und Solaris: /opt/drwcs/Installer/ /opt/drwcs/webmin/install • Für FreeBSD: /usr/local/drwcs/Installer/ /usr/local/drwcs/webmin/install

Bei der Deinstallation des **Servers** der Version **10.0** werden die Konfigurationsdateien im Standardverzeichnis für Sicherungskopien gespeichert:

Datei	Erläuterung	Standardverzeichnis
agent.key (der Name kann abweichen)	Lizenzschlüssel des **Agents**	/var/tmp/drwcs/
certificate.pem	SSL-Zertifikat	
download.conf	Netzwerkeinstellungen für die Generierung der Installationspakete des **Agents**	
drwcsd.conf (der Name kann abweichen)	Konfigurationsdatei des **Servers**	
drwcsd.pri	Privater Schlüssel	
enterprise.key (der Name kann abweichen)	Lizenzschlüssel des **Servers**. Die Datei wird gespeichert, falls sie nach der Aktualisierung von älteren Versionen geblieben ist. Die Datei fehlt im neuen **Server 10.0**.	
frontdoor.conf	Konfigurationsdatei für das Dienstprogramm zur Ferndiagnose des **Servers**	
private-key.pem	Privater RSA-Schlüssel	
webmin.conf	Konfigurationsdatei des **Verwaltungscenters**	
common.conf	Konfigurationsdatei (für einige UNIX-ähnliche Betriebssysteme)	
local.conf	Einstellungen vom Protokoll des **Servers**	
dbexport.gz	Datenbank exportieren	
drwcsd.pub	Öffentlicher Schlüssel	

Bei der automatische Aktualisierung der Software unter **Linux Solaris** werden auch die folgenden Dateien gespeichert:

Für den **Server 6.X**:

Datei	Erläuterung	Standardverzeichnis
auth-ldap.xml	Konfigurationsdatei für die externe LDAP-Autorisierung der Administratoren	/var/opt/drwcs/etc
auth-radius.xml	Konfigurationsdatei für die externe RADIUS-Autorisierung der Administratoren	

Für den **Server 10.0**:

Datei	Erläuterung	Standardverzeichnis
`auth-ldap.xml`	Konfigurationsdatei für die externe LDAP-Autorisierung der Administratoren	`/var/tmp/drwcs/`
`auth-pam.xml`	Konfigurationsdatei für die externe PAM-Autorisierung der Administratoren	
`auth-radius.xml`	Konfigurationsdatei für die externe RADIUS-Autorisierung der Administratoren	

Wenn Sie die Konfigurationsdateien des **Servers** der vorherigen Version verwenden wollen, beachten Sie das Folgende:

1. Lizenzschlüssel des **Servers** werden nicht mehr verwendet (mehr dazu finden Sie unter Lizenzierung).
2. Die eingebettete Datenbank wird aktualisiert, und die Konfigurationsdatei des **Servers** wird mithilfe des Installationsprogramms konvertiert. Diese Dateien müssen beim Update des **Servers** auf die Version **10.0** nicht ersetzt werden.

Datenbank speichern

Wir empfehlen Ihnen, vor der Aktualisierung der Software von **Dr.Web Enterprise Security Suite** eine Sicherungskopie der Datenbank zu erstellen.

So speichern Sie Ihre Datenbank

1. Beenden Sie den **Server**.
2. Exportieren Sie die Datenbank in die Datei:
   - Für FreeBSD:
     ```
     # /usr/local/etc/rc.d/drwcsd.sh exportdb /var/drwcs/etc/esbase.es
     ```
   - Für Linux:
     ```
     # /etc/init.d/drwcsd exportdb /var/opt/drwcs/etc/esbase.es
     ```
   - Für Solaris:
     ```
     # /etc/init.d/drwcsd exportdb /var/drwcs/etc/esbase.es
     ```

Es empfiehlt sich, für die **Server**, die eine externe Datenbank verwenden, die mit der Datenbank mitgelieferten Tools zu verwenden.

Stellen Sie sicher, dass die Datenbank von **Dr.Web Enterprise Security Suite** erfolgreich exportiert wurde. Wenn keine Sicherungskopie der Datenbank erstellt wurde, können Sie den **Server** nicht mehr wiederherstellen.

Automatische Aktualisierung

Bei der Aktualisierung des **Servers** von der Version **6.0** und höher auf die Version **10.0** ist für **Linux** und **Solaris** ein automatisches Upgrade des **Servers** möglich. Starten Sie dafür die Installation des entsprechenden Pakets des **Servers**.

Alle automatisch gespeicherten Dateien werden ebenfalls automatisch konvertiert und in die jeweiligen Verzeichnisse verschoben.

Manuelle Aktualisierung

So aktualisieren Sie den Dr.Web Server bei der Verwendung einer eingebetteten Datenbank

1. Beenden Sie den **Server**.
2. Wenn Sie einige Dateien (außer den Dateien, die automatisch bei der Deinstallation des **Servers** im Schritt **4** gespeichert werden) weiterhin verwenden wollen, erstellen Sie manuell Sicherungskopien dieser Dateien.
3. Löschen Sie den ganzen Inhalt des Repository.
4. Deinstallieren Sie die Software des **Servers** (mehr dazu finden Sie unter Dr.Web Server unter Betriebssystemen der UNIX®-Familie deinstallieren). Sie werden dabei automatisch aufgefordert, Sicherungskopien der Dateien zu speichern. Geben Sie dafür das gewünschte Verzeichnis an oder wählen Sie das vorgeschlagene Verzeichnis aus.
5. Installieren Sie den **Dr.Web Server** der Version **10.0** wie unter Dr.Web Server unter Betriebssystemen der UNIX®-Familie installieren beschrieben, indem Sie die im Schritt **4** erstellte Sicherungskopie verwenden. Alle gespeicherten Konfigurationsdateien und die eingebettete Datenbank werden für den **Server** der Version **10.0** automatisch konvertiert. Nicht konvertierte Datenbank und Konfigurationsdateien des **Servers** älterer Versionen können nicht mehr verwendet werden.

   Wenn Sie einige Dateien manuell gespeichert haben, müssen Sie diese in ihre ursprünglichen Verzeichnisse zurückkopieren.

   Alle gespeicherten Dateien der vorherigen Version des **Servers** (s. den Schritt **6**) müssen im Besitz des Benutzers genommen werden, der bei der Installation der neuen Version des **Servers** ausgewählt wurde (standardmäßig ist das **drwcs**).
6. Starten Sie den **Server**.
7. Konfigurieren Sie die Aktualisierung des Repository und aktualisieren Sie es anschließend.
8. Starten Sie den **Server** neu.

So aktualisieren Sie den Dr.Web Server bei der Verwendung einer externen Datenbank

1. Beenden Sie den **Server**.
2. Wenn Sie einige Dateien (außer den Dateien, die automatisch bei der Deinstallation des **Servers** im Schritt **4** gespeichert werden) weiterhin verwenden wollen, erstellen Sie manuell Sicherungskopien dieser Dateien.
3. Löschen Sie den ganzen Inhalt des Repository.
4. Deinstallieren Sie die Software des **Servers** (mehr dazu finden Sie unter Dr.Web Server unter Betriebssystemen der UNIX®-Familie deinstallieren). Sie werden dabei automatisch aufgefordert, Sicherungskopien der Dateien zu speichern. Geben Sie dafür das gewünschte Verzeichnis an oder wählen Sie das vorgeschlagene Verzeichnis aus.
5. Installieren Sie den **Dr.Web Server** der Version **10.0** wie unter Dr.Web Server unter Betriebssystemen der UNIX®-Familie installieren beschrieben.

6. Verschieben Sie die automatisch gespeicherten Dateien (s.oben):
   - Für **Linux**:

   ins Verzeichnis `/var/opt/drwcs/etc`, `pub`-Schlüssel ausgenommen. Dieser Schlüssel muss in die Verzeichnisse `/opt/drwcs/Installer/` und `/opt/drwcs/webmin/install` verschoben werden.
   - Für **FreeBSD**:

   ins Verzeichnis `/var/drwcs/etc`, `pub`-Schlüssel ausgenommen. Dieser Schlüssel muss in die Verzeichnisse `/usr/local/drwcs/Installer/` und `/usr/local/drwcs/webmin/install` verschoben werden.
   - Für **Solaris**:

   ins Verzeichnis `/var/drwcs/etc`, `pub`-Schlüssel ausgenommen. Dieser Schlüssel muss in die Verzeichnisse `/opt/drwcs/Installer/` und `/opt/drwcs/webmin/install` verschoben werden.

   Wenn Sie einige Dateien manuell gespeichert haben, müssen Sie diese in ihre ursprünglichen Verzeichnisse zurückkopieren.

Alle gespeicherten Dateien der vorherigen Version des **Servers** (s. den Schritt **6**) müssen im Besitz des Benutzers genommen werden, der bei der Installation der neuen Version des **Servers** ausgewählt wurde (standardmäßig ist das **drwcs**).

7. Führen Sie die folgenden Befehle aus:
   - Für **Linux** und **Solaris**:

   ```
   /etc/init.d/drwcsd upgradedb
   ```
   - Für **FreeBSD**:

   ```
   /usr/local/etc/rc.d/drwcsd.sh upgradedb
   ```
8. Starten Sie den **Server**.
9. Konfigurieren Sie die Aktualisierung des Repository und aktualisieren Sie es anschließend.
10. Starten Sie den **Server** neu.

Nachdem die **Server** des Antivirus-Netzwerks aktualisiert wurden, müssen die Verschlüsselungs- und Komprimierungseinstellungen auf den verbundenen **Servern** (mehr dazu finden Sie im **Administratorhandbuch** unter Verbindungen zwischen Servern konfigurieren) neu konfiguriert werden.

4.3. Browser-Erweiterung für das Dr.Web Sicherheitscenter aktualisieren

Um die Browser-Erweiterung für das **Dr.Web Sicherheitscenter** (wird vom **Verwaltungscenter** verwendet) zu aktualisieren, müssen Sie die aktuelle Version manuell deinstallieren und dann eine neuere Version der Erweiterung für das **Dr.Web Sicherheitscenter** installieren.

Die Deinstallation der Erweiterung wird unter Dr.Web Server unter Windows® deinstallieren und Dr.Web Server unter Betriebssystemen der UNIX®-Familie deinstallieren detailliert beschrieben.

Die Installation wird unter Browser-Erweiterung für das Dr.Web Sicherheitscenter installieren detailliert beschrieben.

4.4. Dr.Web Agents aktualisieren

Nachdem die Software des **Servers** aktualisiert wurde, hängt die weitere Vorgehensweise für das Update der **Agents** vom Folgenden ab:

1. Dr.Web Agents unter Windows® aktualisieren,
2. Dr.Web Agents unter Linux, Android und MAC OS X aktualisieren.

4.4.1. Dr.Web Agents unter Windows® aktualisieren

Automatische Aktualisierung

Die automatische Aktualisierung ist unter Vorbehalt folgender Bedingungen möglich:

1. **Agents** müssen auf den Rechnern installiert werden, die unter einem der vom **Agent** für **Dr.Web Enterprise Security Suite** der Version **10.0** unterstützten Windows-Betriebssysteme laufen (weitere Informationen finden Sie im Dokument **Anhänge** unter Anhang A. Vollständige Liste unterstützter Betriebssysteme).
2. Je nach Einstellungen des **Servers** sind folgende Aktionen bei der automatischen Aktualisierung möglich:
   a) Automatische Aktualisierung wird durchgeführt, wenn bei der Aktualisierung des **Servers** Schlüssel und Netzwerkeinstellungen des vorherigen **Servers** gespeichert wurden.
   b) Automatische Aktualisierung erfordert eine manuelle Konfiguration , falls bei der Aktualisierung des **Servers** neue Schlüssel und Netzwerkeinstellungen des **Servers** festgelegt wurden.

Achten Sie bei der automatischen Aktualisierung auf folgende Besonderheiten:

1. Da Benutzer auf der Workstation nach der Deinstallation des **Agents** nicht zum Neustart aufgefordert werden, muss der Administrator den Neustart selbst initiieren.
2. Im Zeitraum von der Deinstallation der alten Version des **Agents** bis zur Installation einer neueren Version sind die Workstations vor Schadsoftware nicht geschützt.
3. Wenn die Workstation nach der Aktualisierung des **Agents** nicht neu gestartet wurde, kann das Antivirenprogramm nicht voll funktionsfähig sein, da einige Komponenten deaktiviert sind. Der Benutzer wird dabei vom **Agent** aufgefordert, die Workstation neu zu starten.

Automatische Aktualisierung von Agents verläuft folgendermaßen:

1. Sobald der Aktualisierungsvorgang gestartet wurde, wird die alte Version des **Agents** deinstalliert.
2. Die Workstation wird manuell neu gestartet.
3. Eine neue Version des **Agents** wird installiert. Die entsprechende Aufgabe wird im Zeitplan des **Servers** erstellt.
4. Nachdem der **Agent** aktualisiert wurde, stellt die Workstation automatisch eine Verbindung mit dem **Server** her. Im Bereich **Status** des **Verwaltungscenters** wird eine Benachrichtigung angezeigt, die darüber informiert, dass ein Neustart erforderlich ist. Die Workstation muss neu gestartet werden.

Manuell konfigurierbare automatische Aktualisierung von Agents verläuft folgendermaßen:

1. Ändern Sie manuell die Einstellungen für die Verbindung mit dem neuen **Server** und ersetzen Sie auf der Workstation den öffentlichen Schlüssel.
2. Sobald die Einstellungen geändert sind und die Workstation mit dem **Server** verbunden ist, startet die Aktualisierung des **Agents**.

3. Sobald der Aktualisierungsvorgang gestartet wurde, wird die alte Version des **Agents** deinstalliert.
4. Die Workstation wird manuell neu gestartet.
5. Eine neue Version des **Agents** wird installiert. Die entsprechende Aufgabe wird im Zeitplan des **Servers** erstellt.
6. Nachdem der **Agent** aktualisiert wurde, stellt die Workstation automatisch eine Verbindung mit dem **Server** her. Im Bereich **Status** des **Verwaltungscenters** wird eine Benachrichtigung angezeigt, die darüber informiert, dass ein Neustart erforderlich ist. Die Workstation muss neu gestartet werden.

Manuelle Aktualisierung

Wenn die neue Version des **Agents** bei der automatischen Installation aus einem Grund nicht installiert werden konnte, werden keine weiteren Installationsversuche vorgenommen. Die Antivirensoftware wird nicht auf der Workstation installiert, und diese Workstation wird im **Verwaltungscenter** als nicht aktiv angezeigt.

In diesem Fall müssen Sie den Agent selbständig installieren. Nach der Installation des neuen **Agents** müssen die neue und die alte Workstation im **Verwaltungscenter**, in der hierarchischen Liste des Antivirus-Netzwerks zusammengeführt werden.

Die Aktualisierung wird nicht unterstützt

Wenn **Agents** auf den Workstations unter den Betriebssystemen, die vom **Agent** für **Dr.Web Enterprise Security Suite** der Version **10.0** nicht unterstützt werden, installiert sind, wird keine Aktualisierung vorgenommen.

Die unter nicht unterstützten Betriebssystemen laufenden **Agents** können keine Updates (darunter aktualisierte Virendatenbanken) vom neuen **Server** beziehen. Wenn die unter nicht unterstützten Betriebssystemen laufenden **Agents** aus einem Grund weiterhin betrieben werden sollen, müssen Sie die **Server** der entsprechenden alten Versionen im Antivirus-Netzwerk beibehalten. Die **Server** der Version **6.XX** und **Server** der Version **10.0** müssen dabei ihre Updates unabhängig voneinander beziehen.

Empfehlungen für die Aktualisierung der **Agents**, die auf LAN-Servern installiert sind, finden Sie im Dokument **Anhänge** unter Agents auf LAN-Servern aktualisieren.

4.4.2. Dr.Web Agents unter Linux, Android und MAC OS X aktualisieren

Agents, die auf Workstations unter Linux-artigen Betriebssystemen, Android oder MAC OS X laufen, können sich mit dem **Server** der Version **10.0** verbinden. Ihr Update ist unter Vorbehalt folgender Bedingungen möglich:

1. **Agents** müssen auf den Rechnern installiert werden, die unter einem der vom **Agent** für **Dr.Web Enterprise Security Suite** der Version **10.0** unterstützten Betriebssysteme laufen (mehr dazu finden Sie im Dokument **Anhänge** unter Anhang A. Vollständige Liste unterstützter Betriebssysteme).
2. Auf den Workstations müssen die Schlüssel und Netzwerkeinstellungen des aktualisierten **Servers** festgelegt sein.

4.5. Proxy-Server aktualisieren

Proxy-Server unter Windows aktualisieren

Eine automatische Aktualisierung des **Proxy-Servers** ist nicht möglich.

Achten Sie beim Start des Installationsprogramms auf einem Rechner mit dem installierten **Proxy-Server** auf das Folgende:

- Wenn die Bitzahl des Installationsprogramms mit der des installierten **Proxy-Servers** übereinstimmt, bekommen Sie eine Meldung, dass die Installation nicht möglich ist.
- Wenn die Bitzahl des Installationsprogramms und die Bitzahl des installierten **Proxy-Servers** unterschiedlich sind, wird der **Proxy-Server** in einem anderen Verzeichnis als dem Verzeichnis der bereits installierten Version installiert.

Zwei **Proxy-Server** dürfen nicht auf dem gleichen Rechner installiert werden und den gleichen Port verwenden, sonst sind die beiden **Proxy-Server** nicht mehr funktionsfähig.

So aktualisieren Sie einen Proxy-Server

1. Wenn auf einem Rechner mit dem **Proxy-Server** der **Dr.Web Agent** mit der aktivierten Selbstschutzfunktion installiert ist, deaktivieren Sie zuerst in den Einstellungen des **Agents** die Komponente **Dr.Web Selbstschutz**.
2. Deinstallieren Sie den **Proxy-Server** wie unter Proxy-Server entfernen beschrieben.

Bei der Deinstallation des **Proxy-Servers** wird auch die Konfigurationsdatei `drwcsd-proxy.xml` (s. dazu im Dokument **Anhänge** den Anhang G4) gelöscht. Speichern Sie bei Bedarf diese Konfigurationsdatei manuell, bevor Sie mit der Deinstallation des **Proxy-Servers** beginnen.

3. Installieren Sie die neue Version des **Proxy-Servers** wie unter Proxy-Server installieren beschrieben.
4. Ersetzen Sie bei Bedarf die Konfigurationsdatei durch die manuell gespeicherte Datei der vorherigen Version.
5. Wenn Sie im Schritt 1 die Komponente **Dr.Web Selbstschutz** deaktiviert haben, aktivieren Sie diese in den Einstellungen des **Dr.Web Agents** erneut.

Proxy-Server unter UNIX-artigen Betriebssystemen aktualisieren

So aktualisieren Sie einen Proxy-Server

1. Bei der Aktualisierung eines **Proxy-Servers** wird auch die Konfigurationsdatei `drwcsd-proxy.xml` (s. dazu im Dokument **Anhänge** den Anhang G4) gelöscht. Speichern Sie bei Bedarf diese Konfigurationsdatei manuell, bevor Sie mit der Aktualisierung des **Proxy-Servers** beginnen.
2. Führen Sie zur Aktualisierung den folgenden Befehl aus:
   `sh ./`*<Distributionsdatei>*`.run`
3. Ersetzen Sie bei Bedarf die Konfigurationsdatei `drwcsd-proxy.xml` durch die vorab manuell gespeicherte Datei der vorherigen Version.

Schlagwortregister

A

Active Directory
- Agent installieren 50
- Deinstallation des Agents 62

Agent
- Deinstallation, active Directory 62
- Deinstallation, für Windows 60
- Installation, Active Directory 50
- Installation, lokale 35
- Installation, remote 42, 47, 50
- Installieren 32, 39
- Update 73

Agent installieren 32
- Active Directory 50
- Installationspaket 36
- Installationsprogramm 39
- lokal 35
- Remote 42, 47, 50

Aktualisierung
- Server, für UNIX 68

Antivirenpaket
- entfernen 60
- Installieren 32, 50

Antivirus-Netzwerk
- Planung 21

B

Basisdistribution des Dr.Web Servers
- Deinstallation, für UNIX 58
- Deinstallation, für Windows 58
- Installation, unter UNIX 29
- Installation, unter Windows 22
- Umfang 18

Browser-Erweiterung für das Dr.Web Sicherheitscenter
- Aktualisierung, für Windows 64
- Deinstallation, für UNIX 59
- Deinstallation, für Windows 58
- Installation 31
- Update 72

D

Deinstallation
- Browser-Erweiterung für das Dr.Web Sicherheitscenter, für UNIX 59
- Browser-Erweiterung für das Dr.Web Sicherheitscenter, für Windows 58

Deinstallation des Agents
- Active Directory 62
- für Windows 60
- Installationspaket, für Windows 61
- Installationsprogramm, für Windows 61

Deinstallation des Dr.Web Servers
- Basisdistribution, für UNIX 58
- Basisdistribution, für Windows 58
- Zusätzliche Distribution, für UNIX 59
- Zusätzliche Distribution, für Windows 58

Demoschlüssel 20

Distribution 18

Distributionsumfang 18

Dr.Web Server
- Aktualisierung, für UNIX OS 68
- Aktualisierung, für Windows 64
- Deinstallation, für UNIX 58
- Deinstallation, für Windows 58
- Installation, unter UNIX 29
- Installation, unter Windows 22

E

entfernen
- Antivirenpaket 60
- Komponenten 60
- Proxy-Server 62

I

Installation
- Browser-Erweiterung für das Dr.Web Sicherheitscenter 31

Installation des Dr.Web Servers
- Basisdistribution, für UNIX 29
- Basisdistribution, für Windows 22
- zusätzliche Distribution des Dr.Web Servers 30

Installationspaket
- Deinstallation, für Windows 61
- Installieren 36
- Umfang 34

Installationsprogramm
- Deinstallation, für Windows 61
- Installieren 39
- Typen 34
- Umfang 34

Installationsseite 34

Installieren
- Antivirenpaket 32

Schlagwortregister

Installieren
NAP Validator 55
Proxy-Server 55

K

Kontos
Workstation, einrichten 36

L

Lizenzierung 19

N

NAP Validator
Installieren 55
Netzwerk-Scanner 47

P

Proxy-Server
entfernen 62
Installieren 55
Update 75

R

Registrierung
des Dr.Web Produktes 19

S

Schlüssel 19
Demo 20
Lizenz erhalten 19
siehe auch Registrierung 19
Symbole
Netzwerk-Scanner 48
Systemanforderungen 14

U

Update
Agent 73
Browser-Erweiterung für das Dr.Web Sicherheitscenter 64, 72
Dr.Web Enterprise Security Suite 64
Proxy-Server 75
Server, für Windows 64

W

Workstation
Benutzerkonto anlegen 36

Z

Zusätzliche Distribution des Dr.Web Servers
Deinstallation, für UNIX 59
Deinstallation, für Windows 58
Installation 30
Umfang 18

© Doctor Web, 2015